

Validierung eines semi-quantitativen Ansatzes zur Risikobeurteilung in der Eisenbahntechnik

Von der
Fakultät Architektur, Bauingenieurwesen und Umweltwissenschaften
der Technischen Universität Carolo-Wilhelmina
zu Braunschweig

zur Erlangung des Grades einer
Doktoringenieurin (Dr.-Ing.)
genehmigte

Dissertation

von
Dipl.-Ing. Sonja-Lara Bepperling (geb. Kurz)
geboren am 04.11.1980
in Düsseldorf

| | |
|----------------------|-------------------|
| Eingereicht am | 27. Juni 2008 |
| Mündliche Prüfung am | 28. November 2008 |

| | |
|------------------|----------------------------|
| Berichterstatter | Prof. Dr. Jens Braband |
| | Prof. Dr. Jörn Pacht |
| | Prof. Dr. Jochen Trinckauf |

2008

Kurzfassung

Die Durchführung von Risikobeurteilungen für Eisenbahnsysteme ist rechtlich und normativ erforderlich. Allerdings werden keine spezifischen Methoden vorgeschrieben, die für Risikobeurteilungen genutzt werden sollen. Bislang fehlen auch spezifische Anforderungskataloge für Risikobeurteilungsmethoden, die beschreiben, welche Eigenschaften solche Methoden erfüllen müssen. Dadurch weisen viele bislang eingesetzte Verfahren zur Risikobeurteilung sowohl in der Konstruktion als auch in der Anwendung erhebliche Schwächen auf.

Die allgemein gehaltenen Vorgaben der europäischen Normen (CENELEC) und der zukünftigen europäischen Gesetzgebung (ERA Recommendation) wurden produktspezifisch angepasst und zur Anwendung einer verbesserten und verfeinerten Methodik zur Risikobeurteilung erarbeitet. Diese Methodik wurde unter dem Produktnamen ‚BP-Risk‘ bereits von Siemens Corporate Technology (CT) und vom Eisenbahnbundesamt (EBA) positiv bewertet.

Die vorliegende Arbeit beschreibt die Erarbeitung einer adäquaten Systemdefinition, auf deren Grundlage das Verfahren BP-Risk angewendet werden soll. Darauf aufbauend wird die Konstruktion von BP-Risk als semi-quantitatives Verfahren detailliert vorgestellt. Alle Annahmen, Modelle und Bewertungskriterien werden dabei offengelegt. Insofern besitzt BP-Risk (im Gegensatz zu den klassischen Methoden) nachweisbare Eigenschaften, was bedeutet, dass ein systematischer Verfahrensnachweis geführt werden kann, da die Methode nachvollziehbar und transparent konstruiert wurde.

Die Kalibrierung der Methode erfolgt anhand eines neuen europäischen Risikoakzeptanzkriteriums, das in der zukünftigen europäischen Gesetzgebung (CSM Recommendation) verankert sein wird. Die Validierung von BP-Risk besteht aus der Nachweisführung bezüglich europäisch gültiger Anforderungen für Risikobeurteilungsmethoden.

Zusätzlich wird BP-Risk für einen neuen Anwendungsfall aus dem Eisenbahnbereich eingesetzt und zeigt somit seine praktische Eignung zur Ableitung von gültigen Sicherheitsanforderungen.

Dieses Dissertationsprojekt liefert den Nachweis, dass BP-Risk korrekt konstruiert ist und gültige Ergebnisse ableitet. BP-Risk ist unter Beibehaltung einer soliden Konstruktion anwenderfreundlich gestaltet. Als semi-quantitativer Ansatz ist BP-Risk einer der ersten begründeten und praktikablen Methoden, die als explizite Risikoanalyse die europäischen Anforderungen erfüllt. Durch die Möglichkeit, die Methodik an spezielle Anwendungsbereiche anzupassen, besitzt BP-Risk das Potential, eine einheitliche Sicherheitsmethode für die gesamte Eisenbahntechnik zu werden.

Abstract

Performing a risk assessment for a new railway system is demanded by law and by industrial standards. However, there are no particular methods or tools specified that have to be used to carry out a risk assessment. Up to now, there are no specific ‘requirement specifications’ for risk assessment methods, which describe the demanded properties. Thus, many risk assessment methods in use so far, show substantial weaknesses in construction and application.

The generic specifications of European standards (CENELEC) and of the oncoming European law (ERA Recommendation) were adapted to create an improved and sophisticated methodology for risk assessments. This approach, labeled as ‘BP-Risk’, was already acknowledged by Siemens Corporate Technology (CT) and by the German Federal Railway Authority (EBA).

The thesis at hand describes the formulation of an adequate system definition, which is the basis for applying the BP-Risk method. Thereupon, the construction of BP-Risk as a semi-quantitative approach is presented and all the assumptions, models and design criteria are revealed. Insofar, BP-Risk features traceable properties, allowing a systematic verification of the process, since the method is comprehensibly and transparently constructed.

The calibration of the method is carried out with a new European risk acceptance criterion, which will be part of the oncoming European law (CSM Recommendation). Subsequently, the validation of BP-Risk comprises the verification in terms of European criteria for risk assessment methods.

In addition, BP-Risk is used for a new railway application to demonstrate its ability to derive valid safety requirements.

This dissertation confirms that BP-Risk is appropriately constructed and that it derives valid results. BP-Risk is user-friendly designed by retaining a solid construction. As a semi-quantitative approach, BP-Risk is one of the first justified and feasible methods, which fulfills the European requirements for explicit risk analysis. Having the potential to adjust the approach to specific application areas, BP-Risk has the potential to become a common safety method for the entire field of railway technology.

Then you will go on your way in safety.

Proverbs 3, 23 (NIV)

Danksagung

Diese Arbeit entstand im Rahmen des Graduiertenkollegs Rail Automation Graduate School (RA:GS!), die von der Rail Automation Academy (RA A) der Siemens AG Division Industry Mobility (ehemals Transportation Systems) im Oktober 2005 gegründet wurde. Das Graduiertenkolleg widmet sich der Forschung von Grundlagenthemen der Eisenbahn-Automatisierungstechnik. Ich danke dem Graduiertenkolleg, das die Durchführung dieser Arbeit in Zusammenarbeit mit der Siemens AG und der TU-Braunschweig ermöglicht hat. Insbesondere bedanke ich mich bei der Siemens AG für die Förderung durch ein Promotionsstipendium.

Mein ganz besonderer Dank gilt meinem Betreuer und Doktorvater Prof. Dr. Jens Braband (Principal Engineer RAMSS und Leiter Research im Bereich Rail Automation der Division Mobility der Siemens AG und Honorarprofessor für Risiko- und Sicherheitsanalysen an der TU Braunschweig), der mir diese Promotion ermöglicht und mich fachlich und persönlich begleitet und mich immer wieder herausgefordert hat.

Meinem Coach an der Hochschule Prof. Dr. Jörn Pacht (Leiter des Instituts für Eisenbahnwesen und Verkehrssicherung an der TU Braunschweig) danke ich für seine Betreuung und fachliches Feedback. Prof. Dr. Jochen Trinckauf (Inhaber der Professur für Verkehrssicherungstechnik an der TU Dresden) danke ich für die externe Berichterstellung. Prof. Dr. Wolfgang Niemeier (Leiter des Instituts für Geodäsie und Photogrammetrie an der TU Braunschweig) danke ich für die Bereitschaft, den Vorsitz der Prüfungskommission zu übernehmen.

Mein herzlicher Dank geht an meine Kollegen bei Siemens I MO RA RD I für ihre fachlichen Rückmeldungen und der freundschaftlichen Zusammenarbeit. Ich bin dankbar für die Möglichkeit, von den jahrelangen praktischen Erfahrungen aus der Industrie profitiert zu haben. Ich danke meinen Kollegen am Institut für Eisenbahnwesen und Verkehrssicherung (IfEV) an der TU Braunschweig, insbesondere Birgit Milius, für die nette Zusammenarbeit und die erfolgreichen gemeinsamen Projekte und Veröffentlichungen.

Besonderer Dank geht an meinen Ehemann Martin, meine Eltern Volkmar und Renate und meinen Bruder Alexander mit seiner Familie sowie an meine Freunde, die mir während des Promotionsstudiums zur Seite gestanden und mich immer wieder unterstützt haben.

Dank sei dem, dem ich alles verdanke!

Braunschweig im Dezember 2008,

Sonja-Lara Bepperling

Inhalt

| | | |
|----------|---|-----------|
| 1 | Einleitung | 14 |
| 1.1 | Begriffe und Vorüberlegungen..... | 14 |
| 1.2 | Problemstellung und Motivation..... | 16 |
| 1.3 | Vorgehensweise | 18 |
| 2 | Risikobeurteilungen für die Eisenbahntechnik | 21 |
| 2.1 | Gesetzliche Randbedingungen | 21 |
| 2.1.1 | Deutschland..... | 21 |
| 2.1.2 | Europa | 22 |
| 2.2 | Normen | 26 |
| 2.2.1 | EN 50126..... | 27 |
| 2.2.2 | EN 50129..... | 27 |
| 2.3 | Begriffe in den Normen und Richtlinien..... | 29 |
| 3 | Methoden zur Risikobeurteilung..... | 30 |
| 3.1 | Quantitative Methoden..... | 31 |
| 3.2 | Qualitative Methoden | 33 |
| 3.3 | Semi-quantitative Methoden..... | 35 |
| 3.4 | Problematik der Bahnindustrie | 37 |
| 3.5 | Zusammenfassung | 39 |
| 4 | Anwendbarkeit | 42 |
| 4.1 | Grundsätzliches..... | 42 |
| 4.2 | Systemdefinition..... | 45 |
| 4.2.1 | prEN0015380-4 | 45 |
| 4.2.2 | Anpassung für BP-Risk | 48 |
| 4.2.3 | Zusätzliche Funktionen..... | 50 |
| 4.3 | Gefährdungsidentifikation aus der Funktionsliste | 52 |
| 4.3.1 | Beispiel: BÜ | 53 |
| 4.3.2 | Exkurs: Allgemein akzeptierbares Risiko | 58 |
| 4.4 | Zusammenfassung | 59 |
| 5 | Best Practice Risk (BP-Risk)..... | 61 |
| 5.1 | Anforderungen..... | 61 |
| 5.2 | Konstruktionsprinzip | 63 |
| 5.3 | Generisches Risikomodell..... | 64 |
| 5.3.1 | Gefahrenabwehr g | 66 |
| 5.3.2 | Schadensausmaß s | 68 |
| 5.4 | Transformation | 69 |

| | | |
|------------|--|------------|
| 6 | Konstruktion | 72 |
| 6.1 | Gefahrenabwehr | 75 |
| 6.1.1 | Betriebliche Randbedingungen | 76 |
| 6.1.2 | Menschliche Gefahrenabwehr..... | 78 |
| 6.2 | Schadensausmaß | 81 |
| 6.2.1 | Maximale Last..... | 82 |
| 6.2.2 | Maßgebliche Geschwindigkeit..... | 83 |
| 6.2.3 | Betroffene Personen..... | 85 |
| 6.2.4 | Exkurs: Bandbreite von S | 88 |
| 6.3 | Zusammenfassung | 90 |
| 7 | Kalibrierung | 92 |
| 7.1 | Europäisches Risikoakzeptanzkriterium | 92 |
| 7.2 | Kalibrierung..... | 94 |
| 7.2.1 | Gefährdungsszenario i_T | 95 |
| 7.2.2 | Gefahrenabwehr G_T | 96 |
| 7.2.3 | Schadenspotenzial S_T | 97 |
| 7.2.4 | Zulässige Versagenshäufigkeit F | 98 |
| 7.3 | Exkurs: Mensch und Technik..... | 99 |
| 7.4 | Zusammenfassung | 102 |
| 8 | Umrechnung..... | 104 |
| 8.1 | Gefährdung an der Systemgrenze..... | 105 |
| 8.2 | Lokale Funktion | 106 |
| 8.3 | Beispiele | 109 |
| 8.3.1 | Bahnübergänge | 109 |
| 8.3.2 | Weiche..... | 113 |
| 8.3.3 | Zentrale Funktion..... | 116 |
| 8.4 | Zusammenfassung | 117 |
| 9 | Validierung | 119 |
| 9.1 | Validierung von BP-Risk..... | 119 |
| 9.2 | Anforderung A01 | 121 |
| 9.3 | Anforderung A02 | 121 |
| 9.4 | Anforderung A03 | 122 |
| 9.5 | Anforderung A04 | 122 |
| 9.6 | Anforderung A05 | 123 |
| 9.7 | Anforderung A06 | 123 |
| 9.7.1 | Risikoformel für individuelles Risiko | 125 |
| 9.7.2 | Formel für kollektives Risiko | 125 |
| 9.7.3 | BP-Risk Model | 129 |

| | | |
|--|--|------------|
| 9.8 | Anforderung A07 | 130 |
| 9.9 | Anforderung A08 | 134 |
| 9.10 | Anforderung A09 | 135 |
| 9.11 | Anforderung A10 | 135 |
| 9.12 | Zusammenfassung | 137 |
| 10 | Neue Anwendung | 139 |
| 10.1 | Zugleitbetrieb | 140 |
| 10.1.1 | Zuglaufmeldungen | 142 |
| 10.1.2 | Fahrwegsicherung | 144 |
| 10.1.3 | Betriebliche Unterlagen | 147 |
| 10.2 | ERA Prozess | 149 |
| 10.2.1 | Systemdefinition | 149 |
| 10.2.2 | Gefährdungsidentifikation | 151 |
| 10.2.3 | Risikoanalyse..... | 153 |
| 10.2.4 | Risikobewertung | 167 |
| 10.3 | Ergebnisse | 169 |
| 11 | Erweiterung..... | 174 |
| 11.1 | Gefährliche Ereignisse mit Reisenden..... | 174 |
| 11.2 | Besetzung der Züge | 178 |
| 12 | Schlussfolgerung | 179 |
| 13 | Zusammenfassung und Ausblick..... | 181 |
| Anhang A: Terminologie | | 183 |
| Anhang B: Abkürzungsverzeichnis | | 187 |
| Anhang C: TSI..... | | 192 |
| Anhang D: Streckenstandards | | 193 |
| Anhang E: Funktionsliste | | 194 |
| Anhang F: Berechnung BÜ..... | | 206 |
| Anhang G: VDV-Schrift 752 | | 207 |
| Anhang H: Funktionen ZLB | | 208 |
| Literaturverzeichnis | | 209 |

Abbildungen

| | |
|---|-----|
| Abbildung 1-1 Funktionale Sicherheit | 15 |
| Abbildung 1-2 Vorgehensweise | 19 |
| Abbildung 2-1 Gesetzpakete der EU im Rahmen der Verkehrspolitik (nach /83/) | 23 |
| Abbildung 2-2 Risiko Management für Common Safety Methods (vereinfacht nach /62/) | 25 |
| Abbildung 2-3 Übersicht über den Prozess aus der EN 50129 (nach /30/) | 28 |
| Abbildung 3-1 Klassifizierung von Risikobeurteilungsmethoden (/93/) | 30 |
| Abbildung 3-2 ASCAP Risikobeurteilung per Monte Carlo Simulation (/86/) | 32 |
| Abbildung 3-3 Risikograph nach VDV 331 (/115/)..... | 33 |
| Abbildung 3-4 Risikomatrix aus der EN 50126 (nach /28/)..... | 34 |
| Abbildung 3-5 Risikomatrix aus der Automobil-Industrie (nach /82/)..... | 35 |
| Abbildung 3-6 Parameter der Risikobewertung für Maschinensicherheit (/76/) | 36 |
| Abbildung 4-1 System (nach /8/, /85/)..... | 43 |
| Abbildung 4-2 Prinzip der Systemdefinition für BP-Risk (nach /9/)..... | 45 |
| Abbildung 4-3 MODTrain Struktur (aus dem Englischen nach /94/) | 46 |
| Abbildung 4-4 Systemdefinition BP-Risk | 50 |
| Abbildung 4-5 Schnittstellenbeschreibung | 51 |
| Abbildung 4-6 Gefährdungsmodell | 52 |
| Abbildung 4-7 Schnittstelle Zug - BÜ | 54 |
| Abbildung 4-8: Unfallursachen an Bahnübergängen (nach /38/)..... | 56 |
| Abbildung 4-9 Allgemein akzeptierbares Risiko (nach /62/) | 58 |
| Abbildung 5-1 BP-Risk Konstruktion..... | 63 |
| Abbildung 5-2: Funktionsversagen des Mensch-Maschine-Systems (nach /9/, S. 100) | 65 |
| Abbildung 6-1 Ablauf der BP-Risk-Analyse..... | 72 |
| Abbildung 7-1 Anwendungsbereich von BP-Risk im Rahmen des ERA-Prozesses | 92 |
| Abbildung 7-2 Sicherheitsziel der Luftfahrt (aus dem Englischen nach /106/) | 93 |
| Abbildung 7-3 Kalibrierung einer Risikomatrix mit RAC-TS (in Anlehnung an /14/)..... | 94 |
| Abbildung 7-4 BP-Risk Prinzip..... | 95 |
| Abbildung 7-5 Versagen von Mensch und Technik (allgemein) | 100 |
| Abbildung 7-6 Kalibrierung mit RAC-TS..... | 101 |
| Abbildung 7-7 Versagen von Mensch und Technik (BP-Risk)..... | 101 |
| Abbildung 8-1 Systemdefinition BP-Risk | 105 |
| Abbildung 8-2 Generischer Fehlerbaum | 105 |
| Abbildung 8-3 Risikomodell für Streckenfunktionen | 109 |
| Abbildung 8-4 Schnittstelle Zug - BÜ | 109 |
| Abbildung 8-5 Fehlerbaum BÜ | 112 |
| Abbildung 8-6 Systemdefinition Weiche | 113 |
| Abbildung 8-7 Fehlerbaum Weiche..... | 114 |
| Abbildung 8-8 Streckenstandard HGV (/37/)..... | 115 |
| Abbildung 9-1 Validierung von BP-Risk | 120 |
| Abbildung 9-2 Ablauf des Nachweises | 124 |

| | |
|---|-----|
| Abbildung 9-3 Von der Gefährdung zum Unfall..... | 127 |
| Abbildung 9-4 kollektives Risiko und BP-Risk Risikomodell im Vergleich | 129 |
| Abbildung 9-5 Rundungsfehler Ausschlag | 133 |
| Abbildung 9-6 Rundungsfehler Toleranzbereich | 133 |
| Abbildung 9-7 absoluter Rundungs- und Einschätzungsfehler | 134 |
| Abbildung 10-1 Grundprinzip des Zugleitbetriebs (nach /97/) | 141 |
| Abbildung 10-2 Trapeztafel (/57/) | 142 |
| Abbildung 10-3 Zuglaufstelle (/118/) | 143 |
| Abbildung 10-4 Rangieren im Zugleitbetrieb (/97/)..... | 144 |
| Abbildung 10-5 Kreuzung auf unbesetztem Bahnhof - Variante 1 (/97/) | 145 |
| Abbildung 10-6 Kreuzung auf unbesetztem Bahnhof – Variante 2 (/97/)..... | 145 |
| Abbildung 10-7 Buchfahrplan (fiktiver Ausschnitt nach /107/, Seite 50) | 147 |
| Abbildung 10-8 Zugmeldebuch (fiktiver Ausschnitt nach /107/, Seite 42)..... | 148 |
| Abbildung 10-9 Fernsprekbuch (fiktiver Ausschnitt nach /107/, Seite 48)..... | 148 |
| Abbildung 10-10 Ursachen der Gefährdungen im Zugleitbetrieb (nach /71/)..... | 151 |
| Abbildung 10-11 Explizite Risikoeinschätzung mit BP-Risk | 154 |
| Abbildung 10-12 Risikobewertung mit BP-Risk..... | 167 |
| Abbildung 10-13 Risikomodell für PZB-Beispiel..... | 170 |
| Abbildung 10-14 Beispiel für Aufteilung der THR..... | 171 |
| Abbildung 11-1 Opfer bei Personenunfällen nach EUROSTAT (/64/) | 176 |
| Abbildung 11-2 Anzahl der Personenunfälle nach EUROSTAT (/64/)..... | 177 |
| Abbildung 12-1 Risiko- und Kritikalitätsbewertung | 179 |

Tabellen

| | |
|---|-----|
| Tabelle 2-1 Terminologie Englisch-Deutsch | 29 |
| Tabelle 3-1 MAIS-Tabelle (aus dem Englischen nach /33/) | 36 |
| Tabelle 3-2 Risikobeurteilungsmethoden im Überblick | 40 |
| Tabelle 4-1 Anforderungen an eine Systembeschreibung | 44 |
| Tabelle 4-2 Funktionen der prEN0015380-4 (Beispiele) | 47 |
| Tabelle 4-3 Transverse Functions (Beispiele)..... | 48 |
| Tabelle 4-4 Funktionsgruppe Zugbeeinflussung | 49 |
| Tabelle 4-5 Anforderungen an Systemdefinition | 49 |
| Tabelle 4-6 Beispiele für zusätzliche Funktionen | 51 |
| Tabelle 4-7 Zusammenfassung funktionale FMEA | 57 |
| Tabelle 5-1 Anforderungen im Vergleich | 61 |
| Tabelle 5-2 Anforderungen für BP-Risk | 62 |
| Tabelle 5-3 Gefährdungsdauer d | 67 |
| Tabelle 6-1 Aufbauprinzip der BP-Risk Tabellen | 74 |
| Tabelle 6-2 Skala für Parameter B..... | 76 |
| Tabelle 6-3 Zusammenstellung der Streckenstandards (vereinfacht nach /37/) | 77 |
| Tabelle 6-4 Menschliche Fehlerraten nach Hinzen (/73/, Seite 62) | 79 |
| Tabelle 6-5 Skala für Parameter M | 81 |
| Tabelle 6-6 Zugpreisklassen (vereinfacht nach /37/) | 82 |
| Tabelle 6-7 Skala für Parameter T | 83 |
| Tabelle 6-8 Skala für Parameter V..... | 85 |
| Tabelle 6-9 Unfälle an Bahnübergängen und Personenschäden im Jahr 2006 (/34/) | 87 |
| Tabelle 6-10: Personenschäden bei Zugfahrten | 88 |
| Tabelle 6-11 Skala für Parameter A..... | 88 |
| Tabelle 6-12 Schadenspotenzial in Anlehnung an /18/ | 89 |
| Tabelle 6-13 Vergleichstabelle zur Spreizung von S..... | 90 |
| Tabelle 7-1 Parameter Betriebsdichte | 96 |
| Tabelle 7-2 Parameter menschliche Gefahrenabwehr | 97 |
| Tabelle 7-3 Parameter Zuggattung | 97 |
| Tabelle 7-4 Parameter maßgebende Geschwindigkeit | 97 |
| Tabelle 7-5 Parameter Unfalltyp | 98 |
| Tabelle 7-6 Skala zur Bestimmung der zulässigen Versagenshäufigkeit | 99 |
| Tabelle 8-1 Durchschnittliche Reisegeschwindigkeiten (nach /1/, /6/, /3/) | 107 |
| Tabelle 8-2 Umrechnungsfaktor | 108 |
| Tabelle 8-3 Funktion LH aus Funktionsliste | 110 |
| Tabelle 8-4 Parameter Betriebsdichte | 110 |
| Tabelle 8-5 Parameter menschliche Gefahrenabwehr | 110 |
| Tabelle 8-6 Parameter Zuggattung | 111 |
| Tabelle 8-7 Parameter maßgebende Geschwindigkeit | 111 |
| Tabelle 8-8 Parameter betroffene Personen..... | 111 |

| | |
|---|-----|
| Tabelle 8-9 Skala zur Bestimmung der zulässigen Versagenshäufigkeit | 112 |
| Tabelle 8-10 Funktion LG | 113 |
| Tabelle 8-11: Verhältnis der Stelleinheiten zu Stellwerken (nach /5/, Seite 8)..... | 116 |
| Tabelle 9-1 Anforderungen für BP-Risk | 120 |
| Tabelle 9-2 Vergleich der Ansätze zur Risikobewertung (aus /9/, Seite 64) | 123 |
| Tabelle 9-3 Relevante Parameter bei BP-Risk | 129 |
| Tabelle 9-4 Zehnerpotenz in der Häufigkeitstabelle | 131 |
| Tabelle 9-5 Einschätzungsfehler | 132 |
| Tabelle 9-6 Rundungsfehler beim Parameter V | 132 |
| Tabelle 9-7 Trade-offs für Risikoparameter | 136 |
| Tabelle 10-1 Betriebliche Funktionen im ZLB | 150 |
| Tabelle 10-2 Gefährdungsliste durch Negation der Systemfunktionen..... | 152 |
| Tabelle 10-3 Betriebliche Gefährdungen des ZLB | 153 |
| Tabelle 10-4 Parameter B für ZLB Beispiel..... | 155 |
| Tabelle 10-5 Parameter T für ZLB Beispiel..... | 156 |
| Tabelle 10-6 Ergebnisse der Risikobewertung | 168 |
| Tabelle 11-1 Durchschnittliche Besetzung der Züge (nach /1/)..... | 178 |
| Tabelle 11-2 Logarithmus für die Besetzung der Züge | 178 |

1 Einleitung

Die vorliegende Arbeit beschreibt die Validierung eines semi-quantitativen Ansatzes zur Risikobeurteilung in der Eisenbahntechnik, genannt Best Practice Risk (BP-Risk).

In diesem ersten Kapitel werden dazu die allgemeinen Begriffe aus dem Bereich der Risikobeurteilung erklärt sowie grundsätzliche Annahmen im Rahmen dieser Arbeit definiert. Des Weiteren wird die Problematik bezüglich der Risikobeurteilungsmethoden erläutert, aus der sich die Motivation und die Zielsetzung dieser Arbeit ergeben haben. Danach werden die einzelnen Schritte des Dissertationsprojektes aufgezählt und näher beschrieben.

1.1 Begriffe und Vorüberlegungen

Das Wort ‚Risiko‘ kommt aus der Seefahrt und bedeutet ursprünglich *„die Klippe, die zu umschiffen ist“* (/67/, Seite 8). Ein Risiko wird im Allgemeinen (/118/) beschrieben als *„die kalkulierte Prognose eines möglichen Schadens bzw. Verlustes im negativen Fall oder eines möglichen Nutzens bzw. Gewinns im positiven Fall“*. Um eine Aussage über Eintrittswahrscheinlichkeit und Verlust- oder Gewinnhöhe möglicher Risiken zu treffen, werden Risikobeurteilungen durchgeführt. Was als Schaden oder Nutzen aufgefasst wird, hängt jedoch von den Wertvorstellungen des Betrachters ab. Da solche Wertvorstellungen stark divergieren, sind auch die Risikobeurteilungen sehr unterschiedlich. Eine Risikobeurteilung versucht im Allgemeinen folgende drei Fragen zu beantworten:

- was kann passieren (Gefahr?),
- wie wahrscheinlich kann die Gefahr eintreten (Eintrittswahrscheinlichkeit?), und
- angenommen, die Gefahr tritt ein, was sind die Konsequenzen (Schadenshöhe?).

Bei einer Risikobeurteilung werden im Rahmen einer systematischen Auswertung aller verfügbaren Informationen Gefahren identifiziert und Risiken abgeschätzt. Nach /11/ sind Risikobeurteilungsmethoden einzusetzen, um beschränkte Ressourcen (z. B. Geld) effektiv zu lenken bzw. Verbesserungspotenziale zu vergleichen. Sie sind nur sinnvoll für Systeme, deren Funktionen und Interaktionen gut verstanden werden (dies gilt nach /11/ in der Regel für Verkehrssysteme).

Risiko ist im allgemeinen Sprachgebrauch das Antonym¹ zu ‚Sicherheit‘. Sicherheit wird in der internationalen Sicherheitsgrundnorm IEC 61508 und dessen sektorspezifische Umsetzung, der EN 50129, definiert als *„Freiheit von unververtretbaren Risiken“*. Hinter dieser Formulierung verbirgt sich die Annahme, dass eine absolute Sicherheit oder Risikofreiheit (bei technischen Systemen) nicht erreicht werden kann. Da komplexe Systeme niemals nachweislich fehlerfrei sind, bzw. nie alle denkbaren Ausfälle beherrscht werden können, muss

¹ Antonyme oder Gegenwörter sind Wörter mit gegensätzlicher Bedeutung.

gesellschaftlich ein gewisses Restrisiko in Kauf genommen werden. Dies wird in der Norm IEC 61508 (sektorspezifisch in den Normen EN 50126 und EN 50129) durch den so genannten risikobasierten Ansatz berücksichtigt. Dieser Ansatz definiert ein tolerierbares Risiko (Risikogrenzwert), das nach Betrachtung aller wirksamen Schutzmaßnahmen unterschritten werden muss.

Die IEC 61508 befasst sich mit der so genannten ‚Funktionalen Sicherheit‘. Funktionale Sicherheit bezeichnet den Teil der Sicherheit eines Systems, der von der korrekten Funktion der sicherheitsbezogenen (Sub-)Systeme und externen Einrichtungen zur Risikominderung abhängt. Dies bedeutet, dass der Bereich der Funktionalen Sicherheit nur einen Teil der Gesamtsicherheit abdeckt (siehe Abbildung 1-1). Nicht zur Funktionalen Sicherheit gehören u. a. elektrische Sicherheit, Brandschutz oder Strahlenschutz. Die vorliegende Arbeit beschränkt sich ausschließlich auf die Aspekte der Funktionalen Sicherheit.

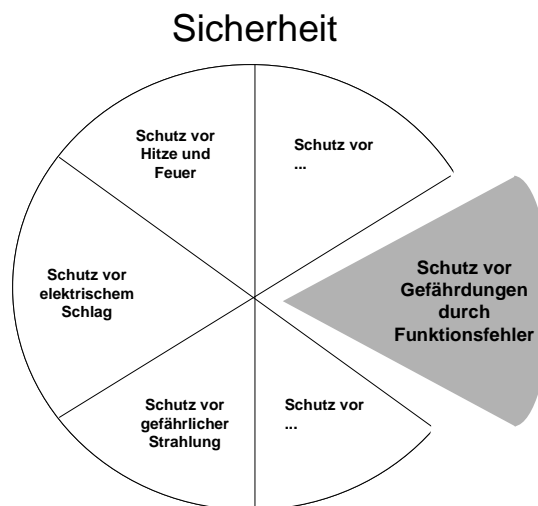


Abbildung 1-1 Funktionale Sicherheit

Einer der am häufigsten genutzten Wege, um (Funktionale) Sicherheit zu erreichen, ist die Ableitung von Sicherheitsanforderungen mit Hilfe von Risikobeurteilungsmethoden. Das Thema Sicherheit darf nach /11/ jedoch nicht isoliert betrachtet werden, z. B. nur für rein technische Funktionen. Betriebliche und auch menschliche Einflüsse müssen einbezogen werden. Es gibt allerdings Faktoren, die zu Unfällen beitragen, aber in Risikobeurteilungen schwer zu fassen sind, z. B. organisatorische Defizite oder Managementbelange. Diese Aspekte sind nur durch Qualitäts- oder Sicherheitsmanagement beherrschbar und werden in dieser Arbeit ebenfalls nicht weiter betrachtet.

In Zukunft wird zum Thema Eisenbahnsicherheit die Sicherheitsrichtlinie der Europäischen Union (EU) eine wichtige Rolle spielen. Sie verlangt die schrittweise Einführung von gemeinsamen Sicherheitszielen (Common Safety Targets²) sowie Sicherheitsanalysemethoden

² Common Safety Target (CST): Sicherheitsniveau, das von verschiedenen Teilen des Eisenbahnsystems mindestens erreicht werden muss, ausgedrückt durch ein Risikoakzeptanzkriterium.

(Common Safety Methods³). Aufgrund von Erfahrungen mit den bisherigen Anwendungsfällen werden für zukünftige Risikobeurteilungen im Rahmen der Common Safety Methods Anforderungen für effiziente Risikobeurteilungsmethoden abgeleitet, die auch zu einer Standardisierung beitragen sollen. Anhand dieser Anforderungen soll ein optimales Verfahren zur Risikobeurteilung gefunden werden. Die vorliegende Dissertation stellt BP-Risk als ein solches optimales Verfahren vor und beschreibt dessen Validierung anhand der genannten europäischen Anforderungen für Common Safety Methods.

Das Wort ‚Validierung‘ oder Validation hat einen lateinischen Ursprung und meint die Prüfung einer These, eines Plans oder eines Lösungsansatzes in Bezug auf das zu lösende Problem. In der Statistik als auch in der Informatik bezeichnet Validierung eine Gültigkeitsprüfung. Bei einem Bezug auf bestimmte Werte wird diese auch Plausibilitätsprüfung genannt. In der EN 50126 wird Validierung definiert als die *„Bestätigung durch Überprüfung und objektiven Nachweis, dass die besonderen Anforderungen für einen spezifischen, bestimmungsmäßigen Gebrauch erfüllt wurden“* (/28/).

Weitere grundlegende Begriffe aus den Normen werden im Anhang dieser Arbeit kurz wiedergegeben und definiert (siehe Anhang A: Terminologie).

1.2 Problemstellung und Motivation

Der risikoorientierte Ansatz, wie er in der IEC 61508 gefordert wird, ist mittlerweile weltweit in fast allen Anwendungssektoren anerkannt und verbindlich (siehe auch /79/). Die Nachteile des risikoorientierten Ansatzes sind jedoch die geringe Bestimmtheit der Anforderungen und der sich daraus ergebende größere Ermessungsspielraum bei der Beurteilung, ob die Anforderungen erfüllt sind. Durch den risikoorientierten Ansatz ist zum Beispiel die in der EN 50129 vorgeschlagene Vorgehensweise zur Risikobeurteilung so flexibel, dass sie bisher auf die aufgetretenen Anwendungsfälle erfolgreich angepasst werden konnte. Die bislang zugesicherten Risikobeurteilungen sind daher fast alle Unikate. Allzu detaillierte Risikobeurteilungen können jedoch vermehrt zu kundenspezifischen, im Extremfall zu streckenspezifischen Lösungen kommen, wenn Risikobeurteilungen zu genau auf spezifische Rand- oder Betriebsbedingungen abgestimmt werden. Dazu sagt das Internationale Technische Komitee (ITC) der Institution of Railway Signal Engineers (IRSE): *„Die Durchführung von separaten Risikoanalysen⁴ für jede einzelne Anlage in einem Land erhöht die Kosten ohne erkennbare Vorteile“* (/81/). Dies würde also dem Gedanken der Kostensenkung durch verstärkte Standardisierung und dem zu fördernden Wettbewerb unter den Anbietern widersprechen.

³ Common Safety Method (CSM): zu entwickelnde Methode, die beschreibt, wie das Sicherheitsniveau und das Erreichen der Sicherheitsziele sowie die Erfüllung von anderen Sicherheitsanforderungen festgestellt wird.

⁴ Die unterschiedlichen Termini in Bezug auf Risikoanalysen und Risikobeurteilungen werden in Kapitel 2.3 erklärt.

Es gilt somit eine Methode zur Risikobeurteilung zu finden, die flexibel, möglichst vielseitig anwendbar und anlagenunabhängig ist. Dies bestätigt die IRSE: „*Es besteht die Möglichkeit zu beträchtlichen Kostenreduzierungen bei Einführung generischer⁵ Analysen.*“ (/81/).

In den Normen werden verschiedene Methoden genannt, die im Rahmen einer Risikobeurteilung angewendet werden können. Sowohl die IEC 61508 als auch die EN 50129 beschreiben sogenannte qualitative Methoden (siehe auch Kapitel 3.2) zur Ableitung von Sicherheitszielen. Ihre unschlagbaren Vorteile bestehen in der Einfachheit und Benutzerfreundlichkeit im Vergleich zu den meisten quantitativen Verfahren (siehe dazu Kapitel 3.1). Allerdings geht man bei quantitativen Methoden i. d. R. über eine generische Beschreibung nicht hinaus, d. h. der Anwender müsste diese Methoden noch anpassen bzw. kalibrieren.

Es gibt z. Z. jedoch für keine qualitative Methode eine veröffentlichte, nachvollziehbare Begründung (oder gar Anleitung), wie die jeweilige Methode erstellt wurde, bzw. welches Grenzkrisiko mit der Benutzung in Kauf genommen wird. Dies ist ein wesentlicher Nachteil und hat schon dazu beigetragen, dass beispielsweise in der Eisenbahnsignaltechnik qualitative Methoden nicht als Standard in die Normen übernommen wurden, obwohl sie z. T. in der Praxis weit verbreitet sind. Eine weitere Schwäche bisher verwendeter qualitativer Methoden besteht darin, dass sie häufig zu konservative Ergebnisse, das bedeutet unnötig hohe Sicherheitsanforderungen, liefern. Die verwendeten Parameter sind relativ grob beschrieben, so dass sich ein großer Ermessensspielraum für den Anwender ergibt und somit die Ergebnisse personengebunden sind. Des Weiteren tendieren die Anwender im Zweifel eher zu ‚worst-case‘ Einschätzungen, um auf der ‚sicheren‘ Seite zu liegen, was ebenfalls zu konservativen Ergebnissen führen kann.

Quantitative Methoden ziehen somit scheinbar den größeren Nutzen aus Risikobeurteilungen, da sie alle Effekte möglichst genau modellieren. Beim Durchführen einer quantitativen Risikobeurteilung wird jedoch erkennbar, dass mit der Anzahl der modellierten Parameter nicht nur der Aufwand steigt, sondern in der Regel die Aussagegenauigkeit des Ergebnisses sinkt, da die für die quantitative Analyse notwendigen Daten nicht in ausreichendem Umfang zur Verfügung stehen.

Aufgrund der hohen Kosten von quantitativen Risikobeurteilungen besteht eine starke Nachfrage bzw. ein gewisser Anwendungsdruck, ein optimales Verfahren zu finden, was die Benutzerfreundlichkeit von qualitativen Methoden mit der exakten/nachvollziehbaren Modellierung von quantitativen Methoden vereint. In der Eisenbahntechnik wurde daher ein neuer Ansatz für eine so genannte semi-quantitative Methode basierend auf den Risikoprioritätszahlen (RPN) vorgeschlagen. Dieser Ansatz wird Best Practice Risk genannt, da es ein aufgrund von Erfahrungen optimales Verfahren zum Thema Risikobeurteilung darstellt.

⁵ Generisch bedeutet hier: möglichst allgemein beschrieben, so dass man das Verfahren für unterschiedliche Anwendungen verwenden kann.

Seine generelle Eignung wurde von Siemens Corporate Technology sowie vom Eisenbahn-Bundesamt (EBA) bestätigt: „BP-Risk wurde bereits intensiv mit zahlreichen Experten, unter anderem der DB AG und des Eisenbahn-Bundesamtes diskutiert. Dabei sind bisher keine Gründe erkannt worden, die einer Verwendung als Methode zur Risikoanalyse in der Eisenbahn-Automatisierungstechnik im Wege stehen“ (/10/).

Die vorliegende Arbeit liefert die Validierung dieses Verfahrens bezüglich europäischer Kriterien für Risikobeurteilungsmethoden. Zusätzlich sollen mit Hilfe von BP-Risk gültige Sicherheitsanforderungen für einen neuen Anwendungsfall abgeleitet werden. Nach /71/ wäre die Ableitung von Sicherheitsanforderungen an die Technik für einfache Sicherungsverfahren, wie z. B. für den Zugleitbetrieb aus einer Risikoanalyse noch ein Forschungsvorhaben. Nach der Definition eines akzeptierten Sicherheitsniveaus wäre die Zulassung der Technik als Sicherheitssystem jedoch möglich und bei erfolgreicher Risikoanalyse wäre eine langfristige Sicherheit gewährleistet. Eine solche Risikoanalyse wird mit Hilfe von BP-Risk am Beispiel des Zugleitbetriebs durchgeführt (siehe Kapitel 10).

Nach derzeitigem Kenntnisstand der Verfasserin gibt es weltweit noch keine Methode, die nach ingenieurwissenschaftlichen Prinzipien konstruiert sowie nachvollziehbar validiert und somit für die Ableitung gültiger Anforderungen eingesetzt wurde. Auf dem Gebiet der Konstruktion nachweislich korrekter Risikobeurteilungsmethoden wäre der BP-Risk Ansatz somit das erste semi-quantitative Verfahren mit veröffentlichtem Nachweis.

1.3 Vorgehensweise

Zunächst werden im Kapitel 2 die gesetzlichen und normativen Randbedingungen für den Einsatz und die Durchführung von Risikobeurteilungen beschrieben. Im Kapitel 3 wird dann der Stand der Technik zum Thema Risikobeurteilungsmethoden dargestellt. Es werden die gebräuchlichen Methoden und Verfahren erläutert und ihre Vor- und Nachteile diskutiert. Aufgrund der oben beschriebenen Motivation, ein optimales Verfahren zu entwerfen, wird im Kapitel 5 das BP-Risk Verfahren vorgestellt. Zuvor wird in Kapitel 4 die Systemdefinition und der Gültigkeitsbereich von BP-Risk beschrieben.

Das Dissertationsprojekt besteht somit aus den folgenden Teilen (siehe Abbildung 1-2):

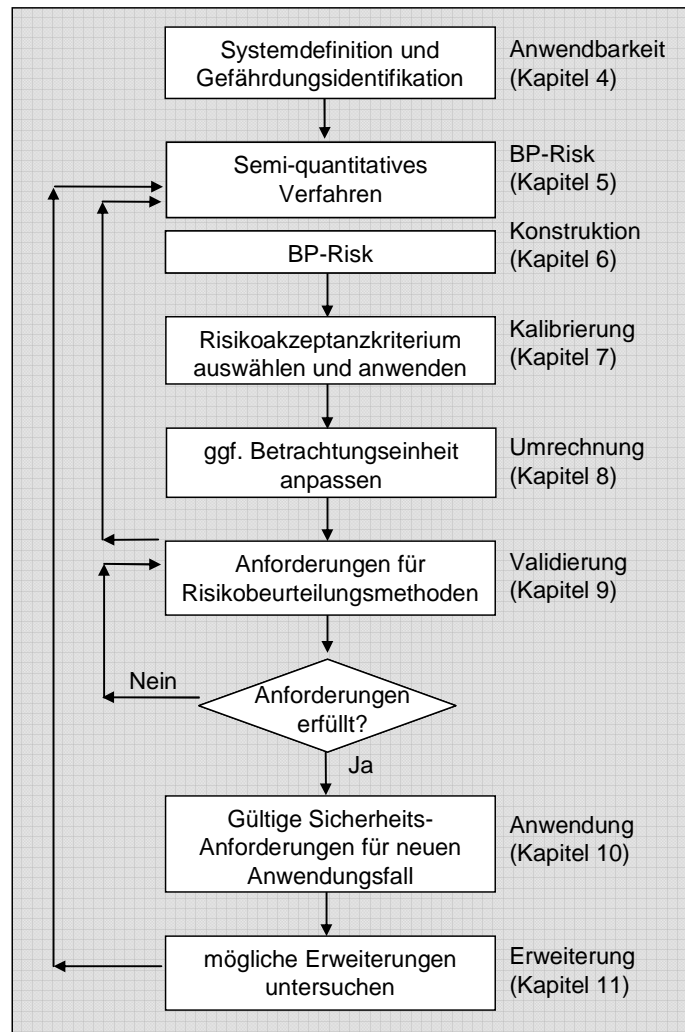


Abbildung 1-2 Vorgehensweise

- **Anwendbarkeit von BP-Risk (Kapitel 4)**

Um BP-Risk möglichst einfach anwenden zu können, muss die Methode anwenderfreundlich und leicht verständlich sowie nachvollziehbar sein. Dazu soll mit einer grundlegenden funktionalen Systemdefinition sichergestellt werden, dass als Ausgangspunkt für BP-Risk eine angemessene Systemebene betrachtet wird.

- **Konstruktion von BP-Risk (Kapitel 5 und 6)**

Eine erste Version für das BP-Risk Verfahren ist bereits veröffentlicht worden (siehe /9/, Seite 97ff). Die Anforderungen an Risikobeurteilungsmethoden haben sich mit Einführung der europäischen Sicherheitsdirektive jedoch geändert. Für die vorliegende Arbeit wurde das BP-Risk Verfahren an die Vorgaben der European Railway Agency (ERA) angepasst. Außerdem war die erste Version des Verfahrens nicht validiert, was im Rahmen dieser Arbeit nun nachgeholt wird.

- **Kalibrierung von BP-Risk (Kapitel 7)**

Es wird gezeigt, wie BP-Risk kalibriert werden kann, indem das Verfahren auf ein europäisches Sicherheitsniveau eingestellt wird. Dabei gilt die Annahme, dass in Europa ein einheitliches betriebliches Sicherheitsniveau vorhanden ist. Gemeinsame Sicherheitsziele werden auf europäischer Ebene angestrebt, so dass ein europäisches Risikoakzeptanzkriterium zur Kalibrierung in BP-Risk implementiert wird.

- **Umrechnung (Kapitel 8)**

BP-Risk basiert auf einem Risikomodell, was einen Zug betrachtet. Die Ergebnisse einer Risikobeurteilung mit BP-Risk müssen jedoch für weiterführende Analysen verwendbar sein und so wird es u. U. nötig, die Bezugseinheit anzupassen. Im Rahmen der Umrechnung wird an ausgewählten Beispielen gezeigt, wie mit Hilfe von Fehlerbäumen und Umrechnungsfaktoren die Versagenhäufigkeiten auf zu realisierende Elemente aufgeteilt werden können.

- **Validierung von BP-Risk (Kapitel 9)**

Es wird bestätigt, dass die Methode BP-Risk die aufgestellten Anforderungen für Risikobeurteilungsmethoden erfüllt, indem ein Befähigungsnachweis erbracht wird. Dabei werden für Europa gültige Anforderungen formuliert und deren Erfüllung durch BP-Risk gezeigt.

- **Ableitung gültiger Sicherheitsziele mit BP-Risk (Kapitel 10)**

BP-Risk wird für ein neues Anwendungsbeispiel angewendet, um gültige Sicherheitsziele abzuleiten. Dazu wird eine Risikobeurteilung für den Zugleitbetrieb (ZLB) mit Hilfe von BP-Risk durchgeführt. Die Risikobeurteilung erfolgt nach dem ERA-Prozess.

- **Erweiterung von BP-Risk (Kapitel 11)**

BP-Risk wurde bereits erfolgreich für andere Anwendungssektoren (z. B. für Turbinensicherheit) angepasst. Zurzeit beschränkt sich BP-Risk noch auf Gefährdungen von Zügen. In dieser Arbeit wird untersucht, wie sich der Ansatz von BP-Risk möglicherweise noch erweitern lässt.

2 Risikobeurteilungen für die Eisenbahntechnik

Risikoforschung ist ein vergleichsweise junges, thematisch vielfältiges und interdisziplinäres Forschungsfeld. Ein gezieltes Interesse an einer systematischen Methodik zur Risikobeurteilung begann in der Raumfahrt im Jahre 1967, als Folge des Unfalls beim Testlauf der Apollo 1, bei dem drei Astronauten ums Leben kamen. Die entwickelten Methoden zur Risikobeurteilung aus dem Raumfahrtprogramm der 1960er Jahre wurden für eine Gesamtanwendung zum ersten Mal in der Kerntechnik eingesetzt. 1975 veröffentlichte die US Nuclear Regulatory Commission (NRC) eine Studie über Reaktorsicherheit, die als erste moderne probabilistische⁶ Risikobeurteilung bezeichnet werden kann (/4/). Wissenschaftliche Risikoabschätzungen finden seither auch in anderen Industriezweigen Verwendung, wie z. B. im Verkehr- und Bauwesen, in der Energiebranche, für chemische Prozesse, in der Luft- und Raumfahrt, im Militärbereich und sogar in der Projektplanung und im Finanzmanagement.

Da der Schwerpunkt der vorliegenden Dissertation auf Risikobeurteilungen in der Eisenbahntechnik liegt, werden zunächst der Risikobeurteilungs-Prozess für die Eisenbahntechnik sowie deren gesetzliche und normative Randbedingungen vorgestellt. Im anschließenden Kapitel 3 werden die wichtigsten Verfahren zur Risikobeurteilung benannt, die zurzeit in der Praxis angewendet werden. Dabei liegt der Fokus auf der Bahntechnik; es werden jedoch auch Verfahren aus anderen Anwendungssektoren (z. B. Automobilindustrie) betrachtet, um die Vergleichbarkeit aufzuzeigen.

2.1 Gesetzliche Randbedingungen

Gesetze sind allgemein verbindliche Rechtsnormen, die vom Gesetzgeber erlassen werden. Bei der Durchführung von Risikobeurteilungen sind die geltenden Gesetze oder Rechtsverordnungen in jedem Fall einzuhalten. Diese werden im Folgenden kurz aufgeführt.

2.1.1 Deutschland

In Deutschland gelten für die Durchführung von Risikobeurteilungen bislang die nationalen Gesetze und Rechtsverordnungen wie die Eisenbahn-Bau- und Betriebsordnung (EBO). Bezüglich der Sicherheit sind die gesetzlichen Vorgaben in Deutschland jedoch relativ allgemein gehalten. Das allgemeine Eisenbahngesetz (AEG) bestimmt in §4 – Sicherheitsvorschriften, Absatz (1): *„Die Eisenbahnen sind verpflichtet, ihren Betrieb sicher zu führen und die Eisenbahninfrastruktur, Fahrzeuge und Zubehör sicher zu bauen und in betriebs sicherem Zustand zu halten.“* (/24/).

⁶ probabilistisch: die Wahrscheinlichkeit berücksichtigend (/89/).

In der EBO §2 – Allgemeine Anforderungen – ist allerdings ein relatives Sicherheitsziel enthalten (/25/). Dieses Kriterium aus Abschnitt (2) wird häufig als ‚Mindestens Gleiche Sicherheit‘ (MGS) bezeichnet:

„(1) Bahnanlagen und Fahrzeuge müssen so beschaffen sein, dass sie den Anforderungen der Sicherheit und Ordnung genügen. Diese Anforderungen gelten als erfüllt, wenn die Bahnanlagen und Fahrzeuge den Vorschriften dieser Verordnung und, so weit diese keine ausdrücklichen Vorschriften enthalten, anerkannten Regeln der Technik entsprechen.

(2) Von den anerkannten Regeln der Technik darf abgewichen werden, wenn mindestens die gleiche Sicherheit wie bei Beachtung dieser Regeln nachgewiesen ist.“

Diese Sicherheitsvorschriften für Deutschland werden in Zukunft schrittweise durch europäische Vorschriften ersetzt werden. Mit Verabschiedung der europäischen Richtlinie über die Eisenbahnsicherheit 2004/49/EG (/52/) wurde bereits die nationale Gesetzgebung in Deutschland angepasst: *„Das Allgemeine Eisenbahngesetz (AEG), die Eisenbahnbetrieblinterverordnung (EBV) und andere Verordnungen wurden geändert sowie die Eisenbahnsicherheitsverordnung (ESiV) und die Eisenbahn-Unfalluntersuchungsverordnung (EUV) neu eingeführt“* (/39/). Weitere Änderungen gelten europaweit ab voraussichtlich September 2008 mit Veröffentlichung der neuen European Railway Agency (ERA) Recommendation für Common Safety Methods (CSM), die im Folgenden kurz vorgestellt wird.

2.1.2 Europa

Die Europäische Kommission hat im Rahmen ihrer Verkehrspolitik in vorerst drei Gesetzespaketen die Förderung insbesondere des grenzüberschreitenden Eisenbahnverkehrs gebündelt (siehe Abbildung 2-1).

Das erste Gesetzeswerk (‚erstes Eisenbahnpaket‘ bestehend aus drei Richtlinien) regelt dabei die Fragen des Zuganges von Fahrwegkapazitäten und Nutzung der Eisenbahninfrastruktur, der Erteilung der Zuweisung von Fahrwegkapazitäten und Nutzung der Eisenbahninfrastruktur. Ergänzend hierzu behandelt das zweite Eisenbahnpaket unter anderem die Entwicklung eines gemeinsamen Sicherheitskonzeptes (Eisenbahnsicherheitsdirektive 2004/49/EG⁷), die Weiterentwicklung der Grundprinzipien der Interoperabilität (Direktive 2004/50/EC) sowie die Schaffung der Europäischen Eisenbahnagentur (Eisenbahnagenturverordnung 881/2004/EC). Das dritte Eisenbahnpaket enthält sowohl Vorschläge insbesondere zur Zertifizierung von Triebfahrzeugführern, zur weiteren Markttöffnung im Schienenpersonenverkehr, flankiert durch Maßnahmen zum Schutz der Rechte von Fahrgästen, als auch Qualitätsvereinbarungen für einen hochwertigen Schienengüterverkehr.

⁷ Mit dem 5. Gesetz zur Änderung eisenbahnrechtlicher Vorschriften wurde Anfang 2007 die Richtlinie 2004/49/EG in nationales Recht umgesetzt.

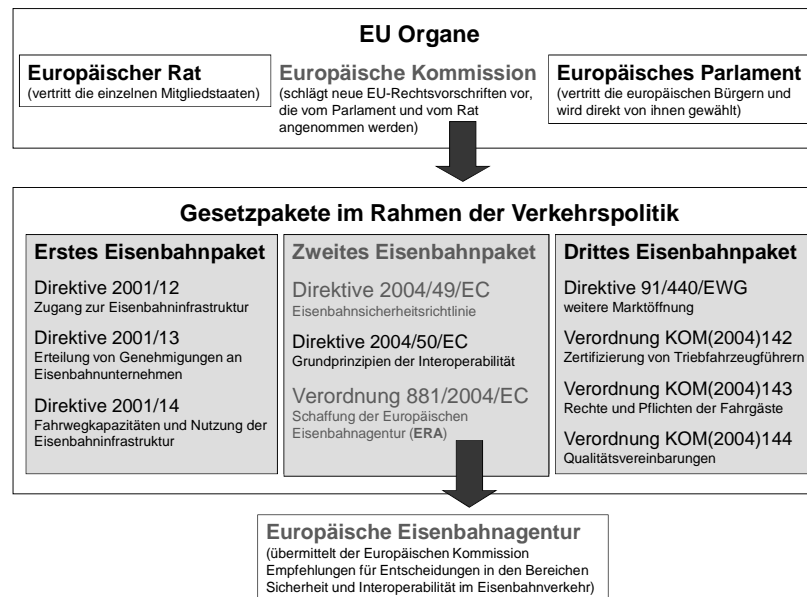


Abbildung 2-1 Gesetzpakete⁸ der EU im Rahmen der Verkehrspolitik (nach /83/)

Auf Grundlage der mit dem zweiten Eisenbahnpaket verabschiedeten Eisenbahnagenturverordnung wurde im Jahre 2004 die Europäische Eisenbahnagentur (ERA) mit Sitz in Valenciennes (Frankreich) gegründet. Aufgabe der Agentur ist es, der Europäischen Kommission Empfehlungen für Entscheidungen in den Bereichen Sicherheit und Interoperabilität im Eisenbahnverkehr zu übermitteln. Im Rahmen dieser Aufgaben erhielt die Agentur durch die Europäische Kommission das Mandat - unter Beachtung der Sicherheitsdirektive - Vorschläge für gemeinsame Sicherheitsziele (CST) sowie Sicherheitsanalysemethoden (CSM) zu erarbeiten. Da es bei der vorliegenden Arbeit um Risikobeurteilungsmethoden geht, werden im Folgenden die Vorgaben insbesondere der CSM näher betrachtet.

Nach Artikel 6, §3 der EU-Sicherheitsdirektive sollen CSMs beschreiben, wie das Sicherheitsniveau und das Erreichen der Sicherheitsziele in Übereinstimmung mit anderen Sicherheitsanforderungen, durch die Ausarbeitung und Festlegung von Risikobeurteilungsmethoden, festgelegt werden. Zusätzlich fordert Artikel 6, §2, dass entworfene CSMs auf der Beurteilung von existierenden Methoden der Mitgliedstaaten basieren sollen. Aus den Anforderungen der Sicherheitsdirektive ergibt sich, dass die Kommission plant, im September 2008 die Methoden für die Ermittlung und Bewertung von Risiken nach einem festgesetzten Verfahren zu erlassen. Diese Verordnung wird voraussichtlich im Januar 2010 verbindlich eingeführt werden und hat dann Gesetzescharakter.

⁸ EG-Richtlinie (engl. Directive): Rechtssetzung der Europäischen Gemeinschaft, die an die Mitgliedstaaten gerichtet ist und diese zur Verwirklichung bestimmter Ziele verpflichtet. Die Wahl der Methode dafür bleibt dem einzelnen Mitgliedstaat überlassen, so dass er bei der Umsetzung der Richtlinie einen gewissen Spielraum hat.

EG-Verordnung (engl. Regulation): Rechtsakt der Europäischen Gemeinschaft, der sich an die Europäische Gemeinschaft selbst, an deren Mitgliedstaaten oder an die Bürger der Mitgliedstaaten richtet. Im Gegensatz zur EG-Richtlinie ist die EG-Verordnung unmittelbar wirksam und verbindlich und benötigt keine Umsetzung auf nationaler Ebene.

Nach /27/ ist das Ziel der CSM, den Sicherheitsnachweisprozess für Eisenbahnanlagen und –verfahren, die ‚signifikante Änderungen‘ („*significant changes*“) darstellen, zu harmonisieren und zu erleichtern. Zurzeit wird noch darüber diskutiert, was genau unter dem Begriff ‚signifikante Änderungen‘ zu verstehen ist und wie dieser in der Praxis umzusetzen ist.

Die erste Reihe („*first set*“) der CSMs (/62/) stellen allgemeine Rahmenbedingungen (Grundsätze und Anforderungen auf hoher Ebene) für die verschiedenen Einsatzbereiche von Risikobeurteilungen auf. Verweise auf spezielle Methoden oder Tools für Risikobeurteilungen werden voraussichtlich nur im CSM Leitfaden („*Guidance of use*“) gemacht. Dieser Leitfaden soll durch entsprechende Erläuterungen und Beispiele helfen, die gemeinsamen Sicherheitsmethoden der ersten Reihe in der Praxis anzuwenden. Der bislang vereinbarte Rahmenprozess für Risikobeurteilungen ist vereinfacht in Abbildung 2-2 dargestellt.

Artikel 6 der ersten Reihe der CSM (/59/) beschreibt das iterative Verfahren aus Abbildung 2-2. Der Prozess besteht aus folgenden Bestandteilen:

- Systemdefinition („*system definition*“);
- Risikoanalyse („*risk analysis*“) einschließlich Gefährdungsidentifikation („*hazard identification*“); und
- Risikobewertung („*risk evaluation*“).

Das Verfahren erfolgt in Verbindung mit dem Führen eines Gefährdungsprotokolls („*hazard log*“). Die Evaluierung der Vertretbarkeit des Risikos des Systems, das der Bewertung unterzogen wird, erfolgt unter Verwendung eines oder mehrerer der folgenden Risikoakzeptanzgrundsätze („*risk acceptance principles*“):

- Anwendung der anerkannten Regel der Technik⁹ („*code of practice*“); oder
- Vergleich mit ähnlichen Systemen¹⁰ („*similar reference system*“); oder
- Explizite Risikoeinschätzung („*explicit risk estimation*“).

Diese Risikoakzeptanzgrundsätze haben eine gewichtete Reihenfolge: „*Falls das Risiko für eine bestimmte Gefährdung durch die Anwendung der anerkannten Regeln der Technik nicht auf ein akzeptables Maß gebracht werden kann, werden zusätzliche Sicherheitsmaßnahmen ermittelt, bei denen einer der beiden übrigen Akzeptanzgrundsätze zum Einsatz kommen*“ (/59/, Artikel 8). „*Wenn die Gefährdungen nicht von einem der beiden Risikoakzeptanzgrundsätze abgedeckt werden, die in den Artikel 8 [code of practice] und 9 [similar reference system] beschrieben sind, erfolgt der Nachweis über die Vertretbarkeit des Risikos in Form einer expliziten Risikoeinschätzung und –evaluierung*“ (/59/, Artikel 10).

⁹ ‚Anerkannte Regeln der Technik‘ bezeichnet ein schriftlich niedergelegtes Regelpaket, das bei ordnungsgemäßer Anwendung zum Ausschluss einer oder mehrerer spezieller Gefährdungen zur Anwendung gelangen kann (/59/, Artikel 3).

¹⁰ ‚Referenzsystem‘ bezeichnet ein System, das sich im Betrieb im Hinblick auf ein akzeptables Sicherheitsniveau bewährt hat, und das als Vergleichssystem herangezogen werden kann, wenn ein System, das einer Bewertung unterzogen wird, auf die Vertretbarkeit seiner Risiken geprüft wird (/59/, Artikel 3).

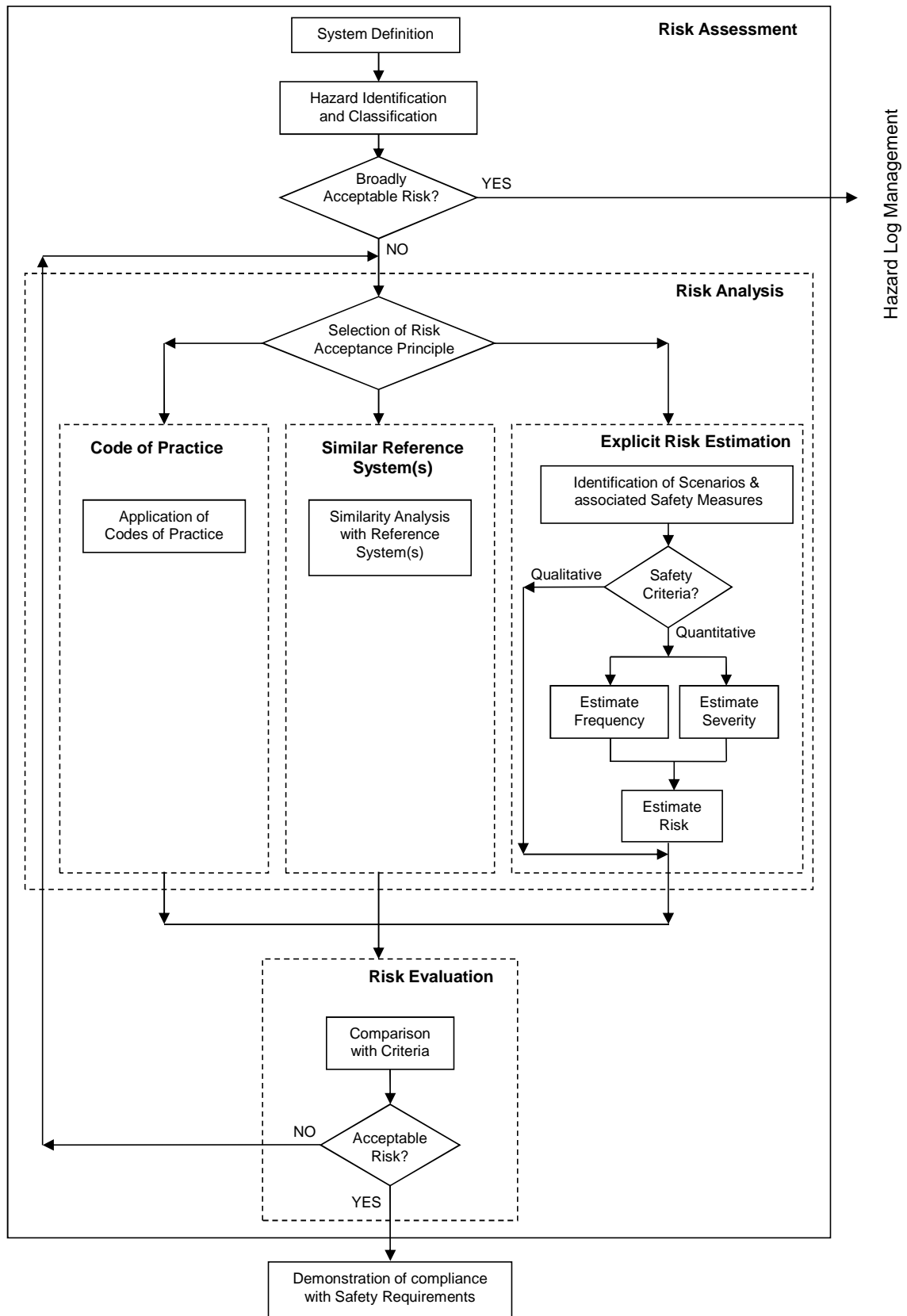


Abbildung 2-2 Risiko Management für Common Safety Methods (vereinfacht nach /62/)

Es muss gezeigt werden, dass der gewählte Risikoakzeptanzgrundsatz angemessen angewendet wird. Das iterative Verfahren ist abgeschlossen, wenn nachgewiesen ist, dass alle Sicherheitsanforderungen eingehalten werden und keine weiteren Gefährdungen zu berücksichtigen sind.

Diese Dokumente der ERA sind bislang in englischer Sprache verfasst, wobei es zurzeit nur eine vorläufige deutsche Übersetzung der CSM-Recommendation gibt (/59/), die jedoch einige Begriffe noch missverständlich übersetzt. Deswegen werden im Rahmen dieser Arbeit vorerst sowohl die englischen Fachbegriffe und Ausdrücke zitiert als auch die deutsche Übersetzung genannt. Wenn die deutsche Übersetzung nicht verwendet wurde, ist kenntlich gemacht, dass das deutsche Zitat aus dem englischen Originaltext von der Verfasserin übersetzt wurde.

2.2 Normen

Dem Anwender von Risikobeurteilungen gibt die Gesetzgebung sehr allgemeine Vorgaben zur Durchführung einer Risikobeurteilung an die Hand. Um einheitliche Eigenschaften von Risikobeurteilungs-Prozessen festzulegen, wurden in Deutschland und auch international Normen erlassen, um dem Anwender vergleichbare und korrespondierende Regeln vorzugeben. Normen sind Standards, die durch Normungsorganisationen veröffentlicht werden. Die Anwendung von Normen ist im Gegensatz zur Einhaltung von Gesetzen freiwillig. Die Arbeitsergebnisse der Normen sind Empfehlungen; erst durch Rechtsakte Dritter können Normen Verbindlichkeit erlangen.

Im Rahmen von Sicherheitsbetrachtungen dominierte in Deutschland bisher in vielen Anwendungsbereichen der regelorientierte Ansatz in den Normen. Dieser besagt, dass eine Anlage sicher ist, wenn gewisse, aus dem Stand der Technik abgeleitete Konstruktionsregeln, eingehalten werden. So wird z. B. in den ‚Technischen Grundsätzen für die Zulassung von Sicherungsanlagen‘ (Mü8004) Sicherheit wie folgt definiert: *„Bei Einhaltung aller Regeln wird die Anlage als ausreichend sicher angesehen, andernfalls nicht“* (/55/).

In den 1990er-Jahren wurde als Teil der Harmonisierung in Europa eine Reihe von Europäischen Normen für den gesamten Eisenbahnbereich geschaffen. So sind entsprechende deutsche Normen bis 2004 zurückgezogen worden und durch die internationale Norm IEC 61508 oder entsprechende sektorspezifische Anpassungen – wie die europäischen CENELEC-Normen EN 50129 – ersetzt worden. Sie definieren ein System von abgestufter Sicherheit, das auf den Elementen des Risikos basiert. Zusätzlich werden technische Anforderungen und Prozesse zur Festsetzung und Überwachung einer hinreichenden Sicherheit über den gesamten Lebenszyklus einer Eisenbahnanlage oder eines Eisenbahnfahrzeugs festgelegt.

„Bis heute verfügen die Eisenbahnen nur über wenig Erfahrung in der Anwendung dieser neuen risikoorientierten Normen, die sich vollständig von den vormals ingenieurtechnischen regelorientierten Vorgehensweisen der MÜ 8804 unterscheiden, welche bisher die Grundlage für die Entwicklung und Zulassung von Eisenbahnsignaltechnik darstellten“ (/45/). Diese mangelnde Erfahrung mag eine Teilursache sein für die heutige Problematik in der Bahnindustrie bezüglich Risikoanalysen bzw. Risikoanalysemethoden, worauf im Kapitel 3.4 noch näher eingegangen wird. Im Folgenden werden vorerst die beiden europäischen Normen EN 50126 und EN 50129 kurz vorgestellt.

2.2.1 EN 50126

Die europäische Norm EN 50126 (/28/) behandelt Aspekte der Zuverlässigkeit, Verfügbarkeit, Instandhaltung und Sicherheit (RAMS) für Bahnanwendungen und bezieht sich auf das gesamte Eisenbahnsystem. Die EN 50126 definiert den Begriff ‚Risikobeurteilung‘ nicht, sondern legt lediglich fest, was sie beinhalten soll. *„DIN EN 50126 ist selbst nicht in der Lage, den Teilprozess der Risikoanalyse eindeutig zu definieren. Auch ein Application Guide zu dieser Norm ist ebenso wenig in der Lage, Abhilfe zu schaffen“ (/104/).*

Als erster Punkt im Prozess steht die Systemdefinition, die allerdings in der EN 50126 außerhalb der Risikobeurteilung beschrieben wird, jedoch als Voraussetzung für die Analyse nötig ist. Zu Risikobeurteilungen gibt es einen Vorgehensvorschlag mit dem Ziel, vorhandene akzeptierbare Gefährdungsraten für den Betrieb eines Systems einzuführen.

Der Anhang der Norm beinhaltet außerdem Vorschläge für Risikoakzeptanzkriterien, durch die ein vorhandenes Risiko untersucht und beurteilt werden kann. Es ist zu erwarten, dass sich dazu in Zukunft Änderungen ergeben werden, weil die Europäische Sicherheitsdirektive die Definition von gemeinsamen Sicherheitszielen (CST) ankündigt.

2.2.2 EN 50129

Die europäische Norm EN 50129 (/30/) wird angewendet auf alle sicherheitsrelevanten Eisenbahnsignalsysteme. Sie ist im Einklang mit der EN 51026, bezieht sich jedoch nur auf den Teil der Eisenbahnsignaltechnik und nicht auf das gesamte Eisenbahnsystem.

Die EN 50129 beschreibt im Detail, welche Maßnahmen und Dokumentationen für die Erstellung eines Sicherheitsnachweises erforderlich sind. Die Anhänge dieser Norm beinhalten weitere Details über bestimmte Schritte zur Erstellung eines Sicherheitsnachweises. Im Gegensatz zur EN 50126 wird eine Forderung zur Anwendung von exakten tolerablen Gefährdungsraten zur Festlegung von Sicherheitsleveln – abgeleitet von der IEC 61508 - eingeführt.

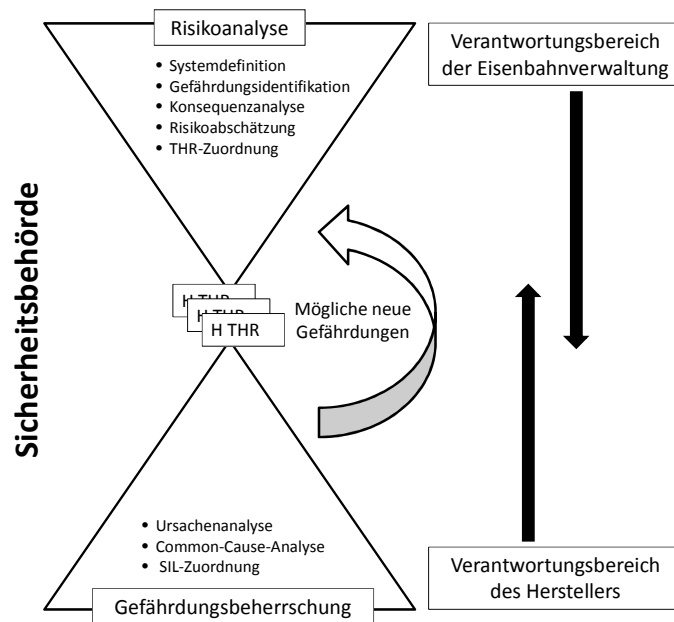


Abbildung 2-3 Übersicht über den Prozess aus der EN 50129 (nach /30/)

Die EN 50129 beschreibt den Sicherheitsanalyse-Prozess anhand einer ‚Sanduhr‘ (siehe Abbildung 2-3). Den Mittelpunkt des Prozesses bildet eine klar definierte Schnittstelle zwischen den Betriebsanforderungen, einschließlich Umgebung, und dem Sicherungssystem als der technischen Lösung. Hinsichtlich der Sicherheit wird diese Schnittstelle durch eine Liste von Gefährdungen bestimmt, die zu einem Unfall führen können. Das Ergebnis der Risikobeurteilung sind Gefährdungsrate (HR), die mit dem System verknüpft sind. Wenn das mit dem System verbundene Risiko geringer ist als der Risikogrenzwert, dann werden diese Gefährdungsrate tolerierbare Gefährdungsrate (THR) genannt.

Es ist die Aufgabe des Betreibers, eine Risikobeurteilung (in der Norm Risikoaanalyse genannt) durchzuführen, die darin besteht,

- die Funktionsanforderungen für das betreffende System (unabhängig von dessen technischer Ausführung) festzulegen,
- systemrelevante Gefährdungen zu identifizieren,
- die Folgen von Gefährdungen zu analysieren,
- sicherzustellen, dass das sich ergebende Risiko tolerierbar ist, und
- die tolerierbaren Gefährdungsrate (THR) abzuleiten.

Der Hersteller ist verpflichtet, eine Gefährdungsanalyse durchzuführen (auch als Gefährdungsbeherrschung bezeichnet), die folgendes umfasst:

- Festlegung der Systemarchitektur unter Berücksichtigung der tolerierbaren Gefährdungsrate für jede Gefährdung,
- Analyse der Ursachen für jede Gefährdung,
- Bestimmung der Sicherheitsanforderung (Sicherheitsanforderungsstufe (SIL) und Gefährdungsrate) für die Teilsysteme,
- Bestimmung der Zuverlässigkeitsanforderungen (Ausfallrate) für das System.

Im Rahmen dieser Arbeit wird nur der zur Risikobeurteilung (siehe Risikoanalyse) gehörige Teil des Sanduhr-Prozesses aus Abbildung 2-3 betrachtet.

Zurzeit läuft eine Überarbeitungsphase der ‚Sicherheitsnormen‘ für die Eisenbahntechnik. Die CENELEC beschloss im Jahr 2006, dass die Gültigkeitsbereiche der signaltechnischen Normen auf Elektrifizierung („Fixed Installations“) und Fahrzeuge („Rolling Stock“) ausgeweitet werden sollen. Geplant ist eine Umstrukturierung der EN 50126 in fünf oder sechs Teile, in denen sich Bestandteile der EN 50129, der EN 50128 (Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme) und EN 50155 (Elektronische Einrichtungen auf Schienenfahrzeugen) wiederfinden sollen. Außerdem sollen die Arbeiten der ERA in das neue Normenpaket EN 50126 (200x) mit einfließen.

2.3 Begriffe in den Normen und Richtlinien

In der EN 50129 werden die Begriffe ‚Risikoanalyse‘ und ‚Risikoabschätzung‘ verwendet. In den Dokumenten der ERA sowie den ISO und IEC Guides kommen die Begriffe „*risk management*“, „*risk assessment*“ sowie „*risk evaluation*“ zur Anwendung. Diese englischen Begriffe dürfen nicht direkt in die deutsche Sprache übersetzt werden, da sie von ihrer Bedeutung her nicht mit den deutschen Begriffen der EN 50129 übereinstimmen. Der Begriff ‚Risikoanalyse‘ aus der EN 50129 ist beispielsweise nicht gleichzusetzen mit „*risk analysis*“, so wie es die ERA verwendet. In dieser Arbeit werden im Folgenden für diese Thematik die deutschen Begriffsdefinitionen aus der IEC 60300 (/78/) verwendet, da diese Definitionen auch für die ERA Dokumente gelten (siehe Tabelle 2-1 und Anhang A: Terminologie).

Tabelle 2-1 Terminologie Englisch-Deutsch

| EN | DE | Bedeutung |
|-----------------|--|---|
| risk management | Risikomanagement | Systematische Anwendung von Managementgrundsätzen, -verfahren und -praktiken zur Analyse, Bewertung und Steuerung/Bewältigung von Risiken. |
| risk assessment | Risikobeurteilung | Gesamtverfahren von Risikoidentifizierung, Risikobeurteilung und Risikobewertung. |
| risk analysis | Risikoanalyse (ohne Systemdefinition!) | Wissenschaftliche systematische Auswertung aller verfügbaren Informationen, um Gefährdungen zu identifizieren und Risiken abzuschätzen. |
| risk estimation | Risikoeinschätzung | Vorgang, durch den ein Maß für die zu analysierenden Risiken erhalten wird; besteht aus den Schritten: Häufigkeitsanalyse, Folgenanalyse und deren Zusammenführung. |
| risk evaluation | Risikobewertung | Abwägung zur Vertretbarkeit eines Risikos auf Grundlage der Risikoanalysen und unter Einbeziehung von sozioökonomischer und umweltbezogener Faktoren. |

3 Methoden zur Risikobeurteilung

Das vorausgegangene Kapitel 2 beschrieb die gesetzlichen und normativen Randbedingungen für den Einsatz und die Durchführung von Risikobeurteilungen. Wie nun die vorgestellten gesetzlichen und normativen Vorgaben in der Praxis umgesetzt werden, stellt das folgenden Kapitel 3 dar, in dem es den Stand der Technik für Risikobeurteilungsmethoden wiedergibt.

Risikobeurteilungen können mit verschiedenen Detaillierungsgraden durchgeführt werden, deren Ausprägungen von der Zielsetzung der Analyse sowie von den verfügbaren Informationen, Daten und Quellen abhängen. Die Methoden zur Risikobeurteilung können eingeteilt werden in:

- 1) quantitativ,
- 2) qualitativ und
- 3) semi-quantitativ.

Eine allgemeine Klassifizierung von Risikobeurteilungsmethoden (/93/) anhand von drei ausgewählten Kriterien bestätigt diese Einteilung (siehe Abbildung 3-1). Hierbei werden semi-quantitative Methoden definiert als qualitative, model-basierte Risikobeurteilungsmethoden. In der Regel lässt sich feststellen, dass der Grad an Komplexität und Kosten der Analyse in der Reihenfolge steigen: qualitativ, semi-quantitativ, quantitativ.

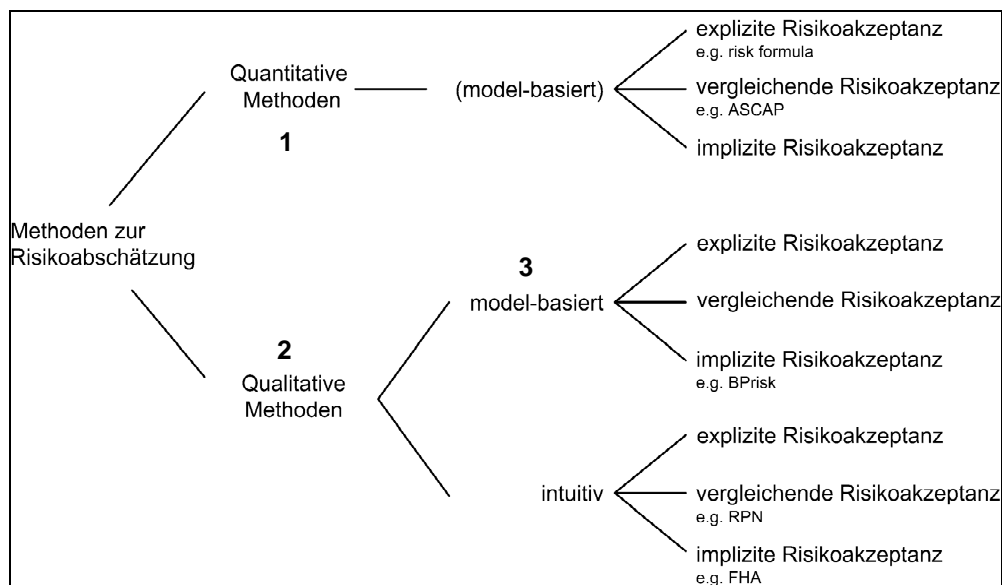


Abbildung 3-1 Klassifizierung von Risikobeurteilungsmethoden (/93/)

Im Folgenden werden diese drei Kategorien von Risikobeurteilungsmethoden erläutert und Beispiele für den jeweiligen Methodentyp kurz vorgestellt.

3.1 Quantitative Methoden

Quantitativ bedeutet „die Quantität betreffend, auf ihr beruhend, mengenmäßig“ (/89/). Quantität betrifft die „Menge, Anzahl oder Umfang“ einer Sache (/89/). Eine quantitative Risikobeurteilung benutzt demnach numerische Werte, um z. B. das Schadensausmaß und/oder die Häufigkeit zu beschreiben. Die Zahlenwerte können durch Simulationen oder Extrapolation von Statistiken bestimmt werden. Die Qualität der Analyse hängt stark von der Genauigkeit und Vollständigkeit der numerischen Werte sowie der Gültigkeit des eingesetzten Verfahrens ab. In Anlehnung an /85/ kann eine quantitative Risikobeurteilung angesehen werden als „empirische Systemanalyse, die die Beziehung zwischen Gefährdungsmaß und Eigenschaften (Variablen) eines Mensch-Maschine-Umwelt Systems (MMUS) auf statistischem Wege und durch die Analyse geschehener Unfälle ermittelt“ (/85/, Seite 5). Als Beispiele für quantitative Methoden werden an dieser Stelle die Risikoformel und der Axiomatic Safety-Critical Assessment Process (ASCAP) kurz beschrieben.

Die Risikoformel dient der allgemeinen Bewertung für individuelle Risiken. Die in der Risikobeurteilung vorkommenden Prozessschritte sowie die benötigten Parameter werden dabei in generischer Form berücksichtigt. Die Risikoformel basiert auf einem heuristischen¹¹ Modell zur Bestimmung des individuellen Risikos, wobei die Zusammenhänge, die von einer Gefährdung zu einem Unfall führen, Berücksichtigung finden (siehe hierzu /20/, /21/, /22/). Die Formel kann entweder durch Verwendung von Mittelwerten oder durch Einsetzen von statistischen Verteilungen für die Parameter ausgewertet werden. Die Risikobewertung erfolgt explizit anhand eines akzeptierten individuellen Risikowerts, der mit dem berechneten vorhandenen individuellen Risiko verglichen wird. Zur BP-Risk Qualifizierung in Kapitel 9.7 wird die unten dargestellte Risikoformel erneut aufgegriffen und noch einmal detaillierter erklärt.

$$IRF_i = N_i \sum_{j=1}^n (HR_j D_j + HR_j E_{ij}) \sum_{k=1}^q (C_{jk} F_{ik})$$

ASCAP ist eine Methode zur Risikobeurteilung, die auf einem ähnlichen Gedankenmodell aufbaut wie die Risikoformel. In ASCAP werden alle zu betrachtenden Prozesse als Markov-Modelle¹² beschrieben. Im Gegensatz zur Risikoformel werden bei ASCAP jedoch die Ergebnisse per Simulation ermittelt. So wird jede Strecke möglichst detailgetreu modelliert (siehe Abbildung 3-2). Dadurch erreicht man einen hohen Detaillierungsgrad, aber gleichzeitig auch einen sehr hohen Aufwand, der bereits von Industrie-Seite bemängelt wurde (/86/). Die Risikobewertung erfolgt anhand einer vergleichenden Risikoakzeptanz. Für das alte und neue System werden mehrere Simulationsläufe unter unterschiedlichen Annahmen durchgeführt, um zu zeigen, ob das neue System mindestens genau so sicher ist wie das alte System. Dies würde im ERA-Prozess einer Risikoanalyse mit Hilfe eines Referenzsystems („similar reference system“) entsprechen.

¹¹ Verfahren, die innerhalb kurzer Zeit und ohne großen Aufwand eine zulässige Lösung liefern.

¹² Stochastischer Prozess, der Wahrscheinlichkeiten für das Eintreten zukünftiger Ereignisse angibt.

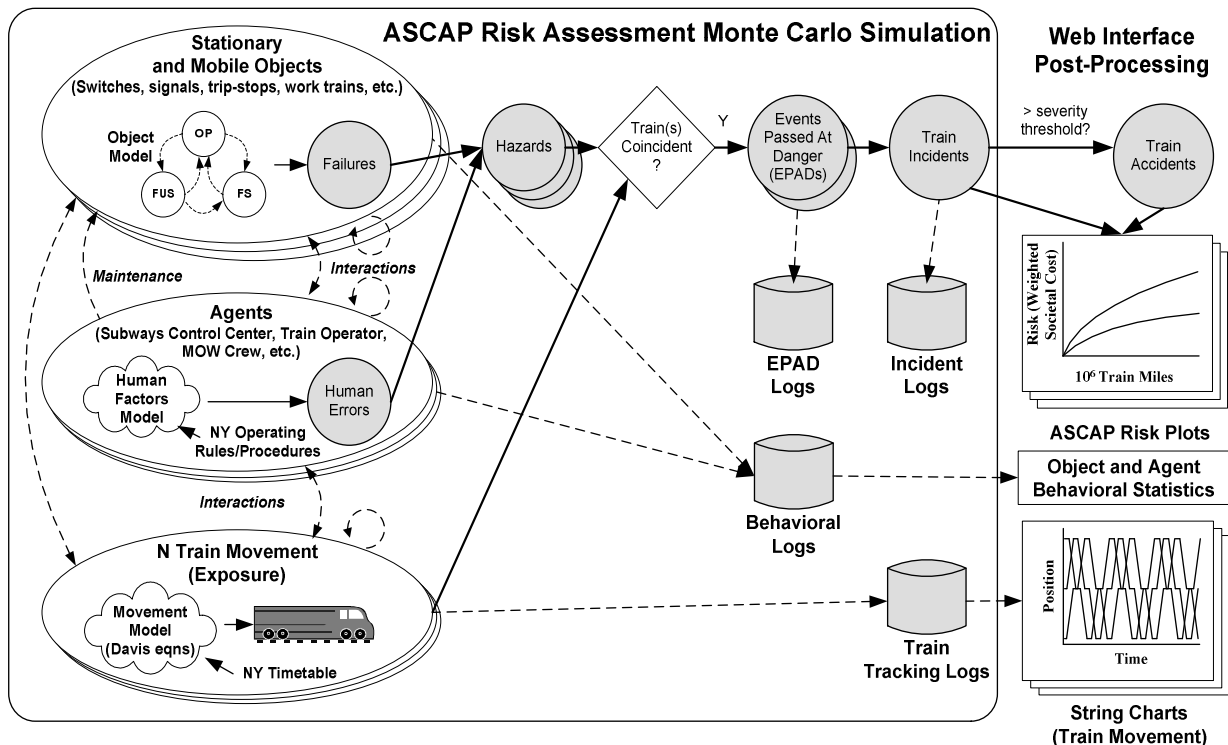


Abbildung 3-2 ASCAP Risikobeurteilung per Monte Carlo Simulation (/86/)

Auf den ersten Blick scheint es, dass man den größten Nutzen aus Risikobeurteilungen dann ziehen kann, wenn man wie bei quantitativen Verfahren alle Effekte möglichst genau modelliert. Erfahrungen aus der Praxis (/9/) zeigen jedoch, dass mit der Anzahl der modellierten Parameter nicht nur der Aufwand und somit die Kosten steigen, sondern in der Regel die Aussagegenauigkeit des Ergebnisses sinkt, da die für die quantitative Analyse notwendigen Daten meist nicht in ausreichendem Umfang zur Verfügung stehen. Dies bestätigt (/85/): „für quantitative Sicherheitsbetrachtungen muss trotz der umfangreichen Instrumente, die von Seiten der Mathematik zur Verfügung stehen, bislang die Erwartung in ihren Erfolg insofern gedämpft werden, als

- notwendige Eingangsdaten vielfach noch nicht zur Verfügung stehen oder
- bei komplexen Mensch-Maschine-Umwelt-Systemen der rechentechnische Aufwand für ein solches Mengenproblem zum Teil unrealistische Vereinfachungen verlangt – und zwar selbst dann, wenn die exakten Wirkungszusammenhänge bekannt sind“ (/85/, Seite 5).

Obwohl in den letzten Jahren zunehmend quantitative Risikoanalysen insbesondere im Bereich der Zulassung elektronischer Einrichtungen Verwendung finden, stellen nach Ansicht der ERA (/83/) quantitative Risikoanalysen nur im Rahmen detaillierter Risikobetrachtungen eine der möglichen Vorgehensweisen dar. Sie sollten insbesondere dann in Betracht gezogen werden, wenn ausreichende Informationen zur Beurteilung der Sicherheit nicht durch die Anwendung eines der beiden anderen Sicherheitsprinzipien („Anerkannte Regel der Technik“ oder „Vergleich mit ähnlichen Systemen“) erlangt werden können.

3.2 Qualitative Methoden

Qualitativ bedeutet „Qualität betreffend, auf ihr beruhend, wertmäßig“ (/89/). Qualität meint in diesem Sinne die „Güte, Wert, oder Beschaffenheit“ (/89/) einer Sache. Qualitative Risikobeurteilungsmethoden benutzen im Gegensatz zu quantitativen Methoden keine realen Zahlen, sondern meist eine verbale Beschreibung, um den Wert des potenziellen Schadens und/oder der Häufigkeit zu beschreiben. Diese verbalen Beschreibungen erfolgen in der Regel anhand von Einteilungen in Kategorien oder Klassen mit Hilfe von Tabellen. Diese Tabellen können meist an bestimmte Randbedingungen angepasst oder erweitert werden. In /85/ werden qualitative Verfahren beschrieben als „theoretische Systemanalyse, die das Gefährdungsausmaß eines MMUS¹³ aus dem Zusammenwirken seiner Komponenten theoretisch ableitet. Dazu gehört die theoretische Analyse möglicher Unfälle“ (/85/, Seite 5). Als Vertreter von qualitativen Methoden werden hier der Risikograph und die Risikomatrix kurz beschrieben.

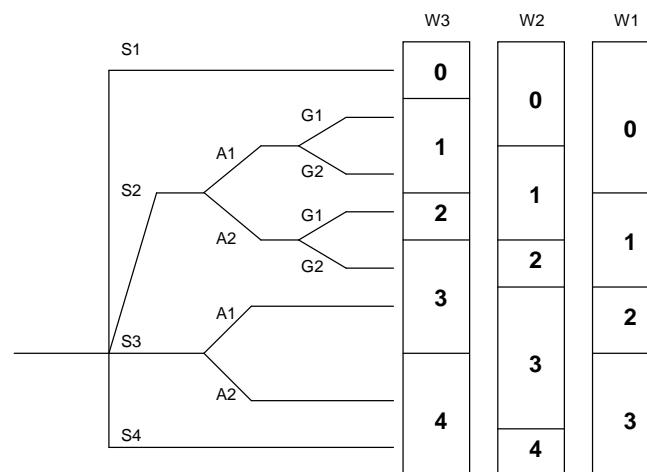


Abbildung 3-3 Risikograph nach VDV 331 (/115/)

Der Risikograph ist eine im Anwendungsbereich der BO Strab (/115/) bewährte Methode der Risikobeurteilung und basiert auf der IEC 61508 Teil 5. Mittels qualitativer Beurteilung von vier Einflussfaktoren wird das notwendige Maß an Risikoreduktion in Form eines SIL¹⁴ (SIL 0 bis SIL 4) für jede Sicherheitsfunktion abgeleitet (siehe Abbildung 3-3). Dabei steht S für Schadensausmaß, A für Aufenthaltsdauer, G für Gefahrenabwehr und W für Wahrscheinlichkeit.

Die wesentlichen Schwächen des Verfahrens liegen darin, dass die Kategorien für die Einflussfaktoren nur verbal beschrieben sind und dass es keine Begründung für die Konstruktion des Verfahrens gibt (/9/, Seite 49).

¹³ MMUS: Mensch-Maschine-Umwelt-System.

¹⁴ SIL: Safety Integrity Level (Sicherheitsanforderungsstufe).

| Häufigkeit eines Gefahrenfalls | Risikostufen | | | |
|--------------------------------|--|------------------|------------------|---------------------|
| Häufig | unerwünscht | intolerabel | intolerabel | intolerabel |
| Wahrscheinlich | tolerabel | unerwünscht | intolerabel | intolerabel |
| Gelegentlich | tolerabel | unerwünscht | unerwünscht | intolerabel |
| Selten | vernachlässigbar | tolerabel | unerwünscht | unerwünscht |
| Unwahrscheinlich | vernachlässigbar | vernachlässigbar | tolerabel | tolerabel |
| Unvorstellbar | vernachlässigbar | vernachlässigbar | vernachlässigbar | vernachlässigbar |
| | unbedeutend | marginal | kritisch | katastrophal |
| | Gefahrenstufen | | | |
| Risikobewertung | Risikominderung/-überwachung | | | |
| intolerabel | muss ausgeschlossen werden | | | |
| unerwünscht | darf akzeptiert werden, wenn eine Risikominderung praktisch nicht durchführbar ist und eine Zustimmung des Bahnunternehmers vorliegt | | | |
| tolerabel | akzeptierbar bei geeigneter Überwachung und mit der Zustimmung des Bahnunternehmers | | | |
| vernachlässigbar | akzeptierbar ohne weitere Zustimmung des Bahnunternehmens | | | |

Abbildung 3-4 Risikomatrix aus der EN 50126 (nach /28/)

In der EN 50126 wird als Beispiel für eine Risikobeurteilung eine Risikomatrix dargestellt (siehe Abbildung 3-4). Bei diesem Verfahren wird eine „Häufigkeit – Konsequenz“ – Matrix gebildet, wobei die Risikokategorien und das Risikoniveau (Risikoakzeptanz) durch den Anwender festgelegt werden müssen. Somit muss die Risikomatrix für jede Anwendung ‚kalibriert‘ (also auf ein gewähltes Sicherheitsniveau eingestellt) werden. Nach /9/ (Seite 52) tendiert der Ansatz dazu, Risiken zu überschätzen, da Anwender häufig von maximalen Werten ausgehen und Risikoreduktionsfaktoren nicht berücksichtigt werden.

Ein weiteres Beispiel für qualitative Methoden sind die Risikoprioritätszahlen (RPN). Sie werden im Eisenbahnwesen eingesetzt, beispielsweise um eine relative Rangordnung für Gefährdungen zu erstellen. Jedoch wurde von /17/ gezeigt, dass dieses Konzept schwerwiegende systematische Fehler aufweist. Trotzdem werden die RPNs als Standard-Ansatz in der Automobil- und Software-Industrie verwendet.

Qualitative Methoden werden im Allgemeinen in der Literatur (z. B. /113/) als nützlich eingestuft, sobald die Daten nicht ausreichend zuverlässig sind, um eine quantitative Modellierung durchzuführen. Bei Anwendern haben qualitative Methoden eine wesentlich höhere Akzeptanz als quantitative Methoden, da sie einfach und schnell anzuwenden sind. Diese Verfahren beruhen jedoch meist auf Erfahrung und haben keine nachvollziehbaren, strengen (konsequenten) Konstruktionsprinzipien. Durch die relativ grobe Beschreibung der Parameter ergibt sich meist ein großer Ermessungsspielraum für den Anwender. Die Gefahr dabei besteht, dass die Bewertungen im Rahmen einer Risikobeurteilung nicht angemessen sind und zu übermäßigen Sicherheitsanforderungen führen.

Diese Einschätzung bestätigen auch ältere Ausführungen zu diesem Thema: „Die qualitative Sicherheitsbetrachtung führt zwar durchaus zu konstruktiven und organisatorischen Sicherheitsmaßnahmen und hat auch in der Vergangenheit die Sicherheitstechnik ständig verbessert, sie lässt aber in der Realisierung technischer Einrichtungen zum Teil einen breiten Spielraum zu. Dieser Spielraum ist in bestimmten Fällen so groß, dass eine Unterordnung der Sicherheitsanforderungen unter das primäre Nutzenziel möglich ist und damit eindeutige Kriterien für die Sicherheit fehlen. Das Sollverhalten unter dem Aspekt der Sicherheit ist dann nur noch ungenau festgelegt“ (/85/, Seite 30).

Da sowohl qualitative als auch quantitative Sicherheitsbetrachtungen ihre Schwächen haben, wurden so genannte semi-quantitative Methoden entwickelt.

3.3 Semi-quantitative Methoden

„Semi...“ hat „als Wortteil in Zusammensetzungen die Bedeutung ‚halb...‘“ (/89/). Semi-quantitativ bedeutet also ‚halb-quantitativ, halb-qualitativ‘. Das heißt, bei semi-quantitativen Risikobeurteilungsmethoden werden den qualitativen Skalen numerische (quantitative) Werte zugeordnet. Somit ist es möglich, einen qualitativen Ansatz zu schaffen, der auf einer ingenieurwissenschaftlichen und nachvollziehbaren Konstruktion beruht.

Beispiele für semi-quantitative Verfahren gibt es in der Automobil-Industrie und in der IEC 62061 für Maschinensicherheit. Der deutsche Verband der Automobilindustrie (VDA) schlägt beispielsweise eine drei-dimensionale Risikomatrix vor (siehe Abbildung 3-5).

| | | | |
|------------------|-----------|-------------------------|----------|
| Exposure: | E4: 1 | Controllability: | C3: 1 |
| | E3: 0,1 | | C2: 0,1 |
| | E2: 0,01 | | C1: 0,01 |
| | E1: 0,001 | | |

| Probability E*C | 1 | 0,1 | 0,01 | 0,001 | 0,0001 |
|-------------------------|----|-----|------|-------|--------|
| S0 - no injuries | QM | QM | QM | QM | QM |
| S1 - MAIS 1-2 | B | A | QM | QM | QM |
| S2 - MAIS 3-4 | C | B | A | QM | QM |
| S3 - MAIS 5-6 | D | C | B | A | QM |

Abbildung 3-5 Risikomatrix aus der Automobil-Industrie (nach /82/)

Der Ansatz basiert auf den drei Parametern:

- Aussetzungsdauer („*exposure*“) E,
- Beherrschbarkeit („*controllability*“) C, und
- Schweregrad („*severity*“) S.

Der Schweregrad wird qualitativ durch eine MAIS („*Maximum Abbreviated Injury Scale*“) Tabelle beschrieben (siehe Tabelle 3-1), während die anderen Parameter quantifiziert werden.

Darum wird dieser Ansatz als semi-quantitativ bezeichnet. Das Ergebnis ist ein automobil-spezifischer SIL (ASIL A bis D). Die Umsetzung dieses Ansatzes erfolgt in der ISO Norm 26262 (zurzeit noch im Entwurf).

Tabelle 3-1 MAIS-Tabelle (aus dem Englischen nach /33/)

| Maximum Abbreviated Injury Scale = Schadensausmaß der schlimmsten Verletzung | | |
|---|------------------|---|
| MAIS 0 | Keine Verletzung | |
| MAIS 1 | Geringfügig | Schürfwunde, Fleischwunde, gebrochener Finger |
| MAIS 2 | Mittelmäßig | einfach gebrochener Knochen, Verlust des Bewusstseins |
| MAIS 3 | Beträchtlich | komplizierter Knochenbruch, Gehirnerschütterung |
| MAIS 4 | Schwer | massive organische Verletzung, Verwundung des Herzens |
| MAIS 5 | Kritisch | Rückenmarksverletzung, gebrochene Gliedmaßen |
| MAIS 6 | Tödlich | Schädelbruch, gebrochener Brustkorb |

Im Maschinensektor (/76/) werden Sicherheitsanforderungen mit Hilfe einer teilweise semi-quantitativen Risikotabelle abgeleitet, welche die Parameter Schadensausmaß (S) und die Wahrscheinlichkeit, dass dieser Schaden eintritt (K), berücksichtigt. K ist eine Funktion von

- der Häufigkeit und der Dauer, wie oft und wie lange die Person einer Gefährdung ausgesetzt ist (F),
- der Wahrscheinlichkeit, dass die Gefährdung eintritt (W), und
- der Wahrscheinlichkeit der Abwehr oder Reduzierung des Schadens (P).

Bei der Klassifikation der Häufigkeit und der Dauer der Exposition (F) werden numerische Werte einer qualitativen Skala (in Form von Klassen) zugeordnet, so dass man diese Tabelle als semi-quantitativ bezeichnen kann.

Das Schadensausmaß wird in vier Kategorien eingestuft, die Wahrscheinlichkeit wird abgeschätzt durch die Addition der drei Subparameter $K = F + W + P$.

Abbildung 3-6 zeigt die Parameter der Risikobewertung für die Maschinensicherheit.

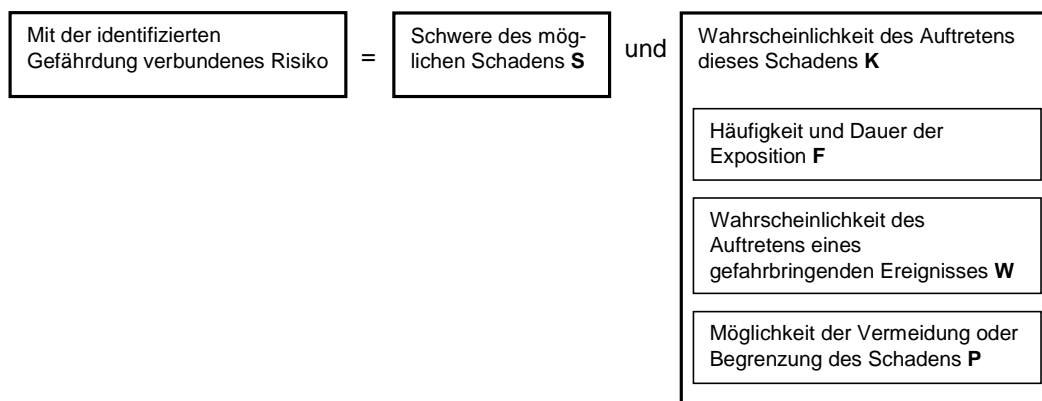


Abbildung 3-6 Parameter der Risikobewertung für Maschinensicherheit (/76/)

Die Vielfalt der bereits vorhandenen und eingesetzten Risikobeurteilungsmethoden sowie deren Unterschiedlichkeiten führen bei Anwendungsfällen in der Praxis oft zu erheblichen Problemen, die im folgenden Abschnitt für den Eisenbahnsektor näher erläutert werden.

3.4 Problematik der Bahnindustrie

Es ist bekannt, dass die Eisenbahn ein hohes Sicherheitsniveau, vergleichbar mit dem aus der Luftfahrt, hat und dass technische Systeme nur einen kleinen Anteil zum betrieblichen Risiko beisteuern (normalerweise um einiges weniger als ein Prozent). Deswegen ist es nach /12/ nicht rentabel, das Sicherheitsniveau von existierenden technischen Systemen oder Sicherheitsfunktionen zu erhöhen, sondern eher dieses hohe Sicherheitsniveau zu vereinheitlichen. *„Eine Benachteiligung des Systems Bahn durch überzogenen Sicherheitsziele soll verhindert werden“ (/83/).*

Um die Harmonisierung der Eisenbahnsicherheit in den europäischen Ländern voranzutreiben, hat die Europäische Kommission im Jahr 2001 die Forschungsprojekte SAMRAIL und SAMNET gestartet. Die European Railway Agency (ERA) hat diese Projekte evaluiert und die wichtigsten Ergebnisse zusammengefasst (/60/). Für den Bereich Common Safety Methods und Risikoanalysemethoden kommt die ERA zu dem Schluss, dass beide Forschungsprojekte einen guten Überblick und eine gute, allgemeine Beschreibung der bekannten Methoden liefern. Jedoch geben sie keine Empfehlung, wie man diese Methoden harmonisiert anwenden kann und definieren auch keine Anforderungskriterien für Common Safety Methods. Die Projekte liefern keine zusätzlichen Informationen im Vergleich zu den Informationen, die schon in zahlreichen Standards vorhanden sind.

Viele Standards und Anwender streben nach relativ einfachen, benutzerfreundlichen Verfahren, insbesondere nach qualitativen oder semi-quantitativen Risikobeurteilungsmethoden. *„Eine unkontrollierte Regelflut und überzogene Anforderungen an Prozesse und technische Ausstattung könnten die Konkurrenzfähigkeit des schienengebundenen Personenverkehrs nachhaltig verschlechtern. Mit anderen Worten: Wir brauchen schlanke und einfach handhabbare Risikoanalyseverfahren mit einem zwar traditionell hohen, aber nicht überzogenen Sicherheitsniveau als Ergebnis“ (/104/).*

Zu diesem Schluss kommt auch die Europäische Kommission, die mit dem Ziel der Markttöffnung für Systeme und Produkte der Eisenbahntechnik in den zurückliegenden Jahren neben der Verabschiedung von Direktiven und Richtlinien auch eine Reihe von Studien und Projekte (wie z. B. SAMRAIL, SAMNET) in Auftrag gegeben hat. Dabei zeigte sich, dass *„die in den Mitgliedsstaaten angewandten unterschiedlichen Verfahrensvorschriften und Sicherheitsphilosophien für die Zulassung von sicherheitsrelevanten Systemen der Eisenbahntechnik zusätzliche Kosten verursachen, die bei Anwendung eines einheitlichen Verfahrens gesenkt und eventuell sogar vermieden werden könnten“ (/83/).*

Es wurde jedoch bis jetzt noch kein optimales Verfahren gefunden. Viel bedenkenswerter als die Kosten ist aber die Tatsache, dass einige der qualitativen Risikobeurteilungsmethoden schwerwiegende Fehler aufweisen, zu konservative Ergebnisse liefern oder keine präzise Beschreibung haben. Vielen der vorhergehend zitierten Methoden fehlen ebenfalls Begründungen, warum sie funktionieren und welche Eigenschaften sie haben. Es fehlt oft eine Anleitung, wie man die Methode konstruiert oder beispielsweise für neue Anwendungsbereiche anpassen kann. In der Bahnindustrie führt diese Situation dazu, dass die Glaubwürdigkeit des risikobasierten Ansatzes untergraben wird. Verschiedene Risikobeurteilungen leiten komplett unterschiedliche Sicherheitsanforderungen ab (selbst innerhalb desselben Landes mit der derselben Sicherheitsbehörde). Für einige neue Systeme dauerte aufgrund dieser Diskrepanz die Debatte über die Sicherheitsanforderungen ein ganzes Jahrzehnt. Allerdings *„scheinen die Diskussionen über richtige Methoden und Verfahren häufig zum Selbstzweck zu werden. Auch die in jüngerer Zeit veröffentlichten Application Guides – von größerem Umfang als die Normenwerke selbst – konnten nur wenig zur Klärung beitragen“* (/104/).

Zurzeit wurde noch keine Methode vorgeschlagen, die eine einfache Anwendung für den Benutzer mit der Strenge oder der Flexibilität einer PRA (Probabilistic Risk Analysis) kombiniert. PRAs (Kategorie: quantitative Risikoanalysemethoden) haben zwar eine mathematische Basis, jedoch zweifeln Experten oft an den Ergebnissen der PRA, aufgrund der mangelnden Glaubwürdigkeit der statistischen Inputdaten. Schon zu Beginn der Entwicklung von Risikobeurteilungen hatte man dies erkannt: *„[...] das Problem von quantitativen Risikobeurteilungen ist, dass wenn Manager Zahlen erhalten, sie diese Zahlen wie absolute Beurteilungen behandeln, ungeachtet der Warnungen, dieses nicht zu tun. Solche Zahlen werden dann als Fakten angenommen, anstatt anzuerkennen, was sie wirklich sind: subjektive Einschätzungen einer Gefährdungsebene und -wahrscheinlichkeit“* (aus dem Englischen nach /4/).

Um vertrauenswürdigeren Eingangsdaten zu erhalten, steigt oft die Datenmenge, was eine PRA wiederum sehr teuer macht. Außerdem wird eine entscheidende Annahme wie Unabhängigkeit oft vernachlässigt, was meist viel zu optimistische Analyseergebnisse ergibt. Deswegen ziehen Fachexperten zumeist qualitative Risikobeurteilungsmethoden (wie Risikomatrizen, Risikographen oder Risikoprioritätszahlen) PRAs vor, da diese Verfahren weniger aufwändig sind und man in Kategorien und nicht in absoluten Zahlen denkt (z. B. Kategorie: katastrophaler Unfall anstatt 57,5 Tote). Um dieses Problem für das deutsche Bahnwesen zu lösen, haben Betreiber, Hersteller, Universitäten und Sicherheitsbehörden eine Diskussion über Anforderungen für Risikobeurteilungsmethoden initiiert, obwohl noch nicht einmal die Methoden vollkommen eindeutig festgelegt sind. Ähnliche Auseinandersetzungen finden in den Arbeitsgruppen der ERA statt. Diese zukünftigen europäischen Vorschriften werden wohl auch keine spezielle Methode empfehlen, sondern lediglich Anforderungen für solche Methoden festlegen. Diese europäischen Anforderungen werden in Kapitel 5.1 kurz wiedergegeben und im Rahmen der Validierung von BP-Risk in Kapitel 9 detaillierter erläutert.

In der Fachwelt wird viel über die Vor- und Nachteile von quantitativen und qualitativen Risikobeurteilungsmethoden diskutiert. Schon zu Beginn der Entwicklung von Risikobeurteilungsverfahren gab es dazu Diskussionen (Zitat aus der Raumfahrtindustrie):

„Es wurde auch klar, dass nicht nur das Misstrauen gegenüber versichernden Risikozahlen der Grund war, warum quantitative Risikobeurteilungen aufgegeben wurden. Vielmehr waren anfängliche Schätzungen von katastrophalen Ausfallwahrscheinlichkeiten so hoch, dass ihre Veröffentlichung die politische Realisierbarkeit gefährdete. [...]. Im Gegensatz dazu [...] waren die qualitativen Methoden, die einfach die Ausfälle identifizierten, die zu einem Unfall führten, insofern eingeschränkt, da nicht alle Teile des betrachteten Systems eine gleiche Gefahr darstellten. Ohne ein Hilfsmittel zur Identifizierung von Ausfallwahrscheinlichkeiten der verschiedenen Teilelemente konnten die Aufmerksamkeit und die Mittel nicht effizient ausgerichtet werden.“ (aus dem Englischen nach /4/).

3.5 Zusammenfassung

Risikobeurteilungsmethoden können nach /93/ in zwei verschiedene Kategorien aufgeteilt werden:

- qualitative oder semi-quantitative Methoden und
- quantitative Methoden.

Der grundlegende Unterschied besteht darin, dass qualitative Methoden das Risiko mit Hilfe einer festgelegten Anzahl von vordefinierten Parametern bewerten, während quantitative Methoden beliebig viele, nicht-vordefinierte Parameter berücksichtigen können. Die offensichtlichen Vorteile von qualitativen oder semi-quantitativen Methoden sind deren einfache Anwendbarkeit und Kosteneffizienz. Der offenkundige Vorteil von quantitativen Methoden ist ihre Flexibilität.

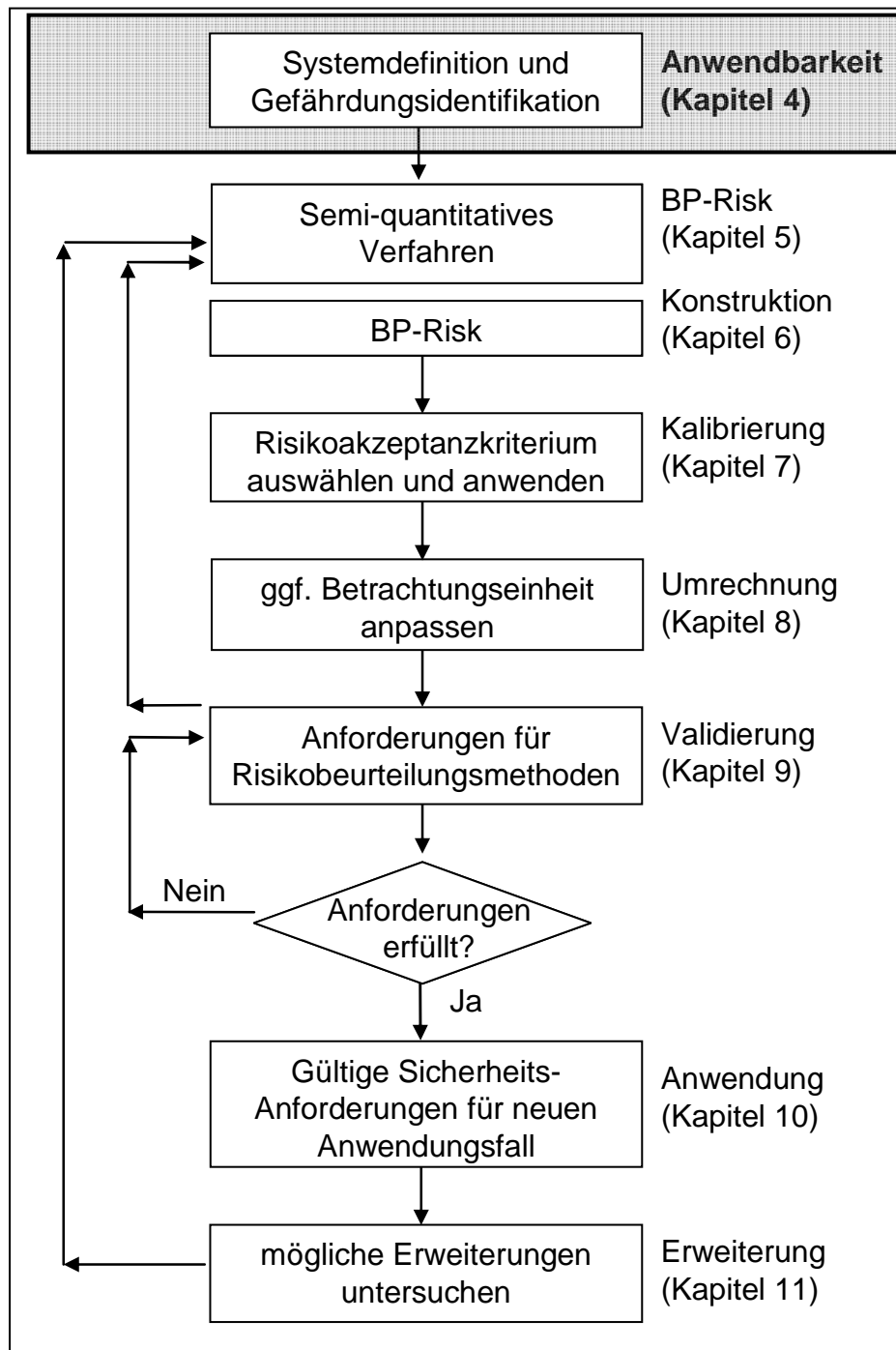
Tabelle 3-2 fasst die beschriebenen Risikobeurteilungsmethoden zusammen, gibt einen Überblick über deren Vor- und Nachteile und nennt die vorgestellten Vertreter der jeweiligen Methodentypen. In /9/ und auch in /105/ werden die gebräuchlichsten Methoden zur Risikobeurteilung ebenfalls zusammengefasst, sowie auf praktischen Erfahrungen basierende Empfehlungen für den Einsatz dieser Methoden gegeben. Fazit aus diesen Betrachtungen ist, dass verwendete Methoden, die oft als Standard-Methoden dargestellt werden, in der Praxis häufig noch fehlerhaft angewendet werden.

Es wurde schon früh klar, dass sowohl quantitative als auch qualitative Methoden zur Risikobeurteilung ihre Schwachpunkte haben. Im Rahmen dieser Arbeit (Kapitel 5 und 6) wird Best Practice (BP)-Risk - das neue semi-quantitative Verfahren für Risikobeurteilung in der Eisenbahntechnik - vorgestellt, was die Stärken von quantitativen und qualitativen Methoden vereint und somit ein optimales Verfahren darstellt.

Tabelle 3-2 Risikobeurteilungsmethoden im Überblick

| Typ | Risiko-Parameter | Vorteile | Nachteile | Beispiele |
|-------------------------|--|---|---|----------------------------------|
| quantitativ | Numerische Werte | Genaue Modellierung | Großer Aufwand, hohe Kosten, detaillierte Daten nötig | Risikoformel, ASCAP |
| qualitativ | Verbale Beschreibung | Einfache, schnelle Anwendung, niedrige Kosten | Zu grobe Parameterbeschreibung, keine Konstruktionsprinzipien | Risikograph, Risikomatrix, RPN |
| semi-quantitativ | Verbale Beschreibung mit numerischen Werten hinterlegt | Einfache, schnelle Anwendung, nachvollziehbare Konstruktion | Keine genaue, Modellierung | ISO 26262 (Entwurf) IEC 62061 |

Bevor eine Risikobeurteilung durchgeführt wird, muss geklärt werden, ob die anzuwendende Methode für die jeweilige Analyse geeignet ist. Der Anwender einer Risikobeurteilungsmethode muss also wissen, für welchen Bereich die einzusetzende Methode gültig ist. Demzufolge ist es notwendig, deutlich herauszuarbeiten, für welche Anwendungsfälle BP-Risk richtige Ergebnisse liefert und wo die Grenzen des Anwendungsbereichs sind. Obwohl der Anwender die Konstruktion der Methode nicht kennen und verstehen muss, ist es wichtig, dass ihm mitgeteilt wird, wann er mit BP-Risk gültige Ergebnisse ableiten kann und wann er möglicherweise die Methode (bzw. deren Parameter) anpassen oder sogar eine andere Methode einsetzen muss. Diese Vorgaben zur Anwendung von BP-Risk werden in Kapitel 4 im Einzelnen beschrieben.



4 Anwendbarkeit

Eine unabdingbare Voraussetzung für jede Risikobeurteilung und somit auch für die Anwendung und Konstruktion von BP-Risk ist das Vorhandensein einer präzisen Systemdefinition, die nicht nur beschreibt, welche Komponenten im System enthalten sind, sondern auch deren Interaktion mit der Umwelt über klar abgegrenzte funktionale Schnittstellen definiert. Die einzelnen Systemfunktionen müssen im Rahmen einer Systemdefinition aufgeführt werden.

Die Anwendung von Risikobeurteilungen sollte nicht auf anlagenspezifischen Systemdefinitionen basieren, um die Nutzung der Resultate in einem weiten Bereich von Anwendungen zu ermöglichen. Darüber hinaus soll im Rahmen von BP-Risk mit einer grundlegenden funktionalen und generischen Systemdefinition sichergestellt werden, dass als Ausgangspunkt für das Verfahren eine angemessene Systemebene betrachtet wird. Auf Grundlage dieser Systemdefinition wird das Verfahren BP-Risk angewendet und auch eine generische Gefährdungsidentifikation ermöglicht.

Im Folgenden werden dazu die grundsätzlichen Schritte einer Systemdefinition vorgestellt und für BP-Risk konkretisiert.

4.1 Grundsätzliches

Sicherheit ist eine Systemeigenschaft (/8/) – was ist also ein System? Dazu gibt es viele Definitionen in zahlreichen Normen. Nach Einschätzung der Verfasserin wird wahrscheinlich niemals eine universelle und eindeutige Definition gelingen. Jeder Systemanalyse muss jedoch eine Bestimmung der Ziele der Analyse vorausgehen. Daraus leiten sich die Definition des Systems sowie die auf das Ziel der Analyse bezogene Systembeschreibung ab. Im Wesentlichen ist folgendes zu leisten (siehe auch Abbildung 4-1):

- Abgrenzung des zu untersuchenden Systems gegen die Umgebung,
- Festlegung, welche Eingangsgrößen aus der Umgebung (Input) und welche Ausgangsgrößen in die Umgebung (Output) wichtig sind,
- Abgrenzung, welche Störeinflüsse aus der Umgebung zu beachten sind,
- Klärung, durch welche Elemente mit welchen Eigenschaften das System beschrieben wird,
- Festlegung, welche Wechselwirkungen zwischen diesen Elementen zu beachten sind.

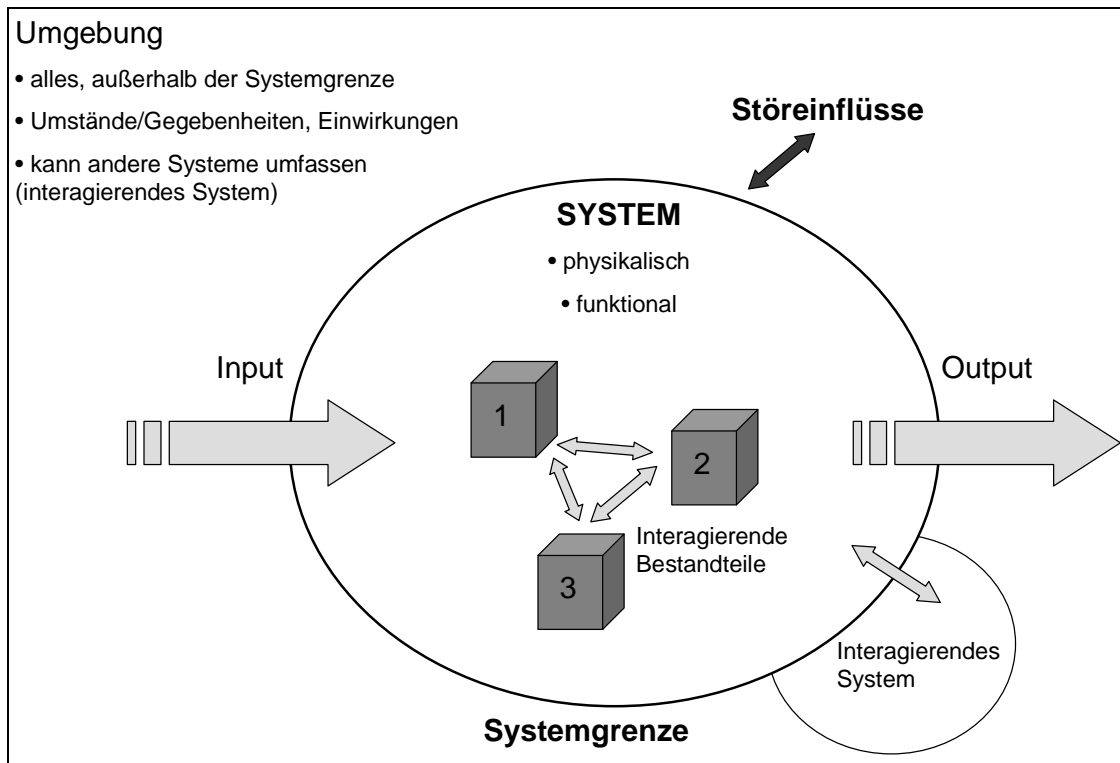


Abbildung 4-1 System (nach [8/, /85/])

Diese allgemeinen Festlegungen finden sich auch bei der ERA wieder. Eine Systemdefinition sollte nach Artikel 6, §2 der CSM-Recommendation mindestens folgende Aspekte berücksichtigen:

- „Definition der Zielsetzung für das System, z. B. beabsichtigte Nutzung;
- Definition der Systemfunktionen und falls relevant auch der Systemelemente;
- Definition von Systemgrenzen einschließlich der interagierenden Systeme;
- Definition der physikalischen und funktionalen Schnittstellen;
- Definition der Systemumgebung;
- Definition der vorhandenen Sicherheitsmaßnahmen sowie Definition der identifizierten Sicherheitsanforderungen aus dem Risikobeurteilungsprozess;
- Definition der Annahmen, welche die Grenzen des Risikobeurteilungsprozesses bestimmen“ (aus dem Englischen nach [62/]).

Es ist davon auszugehen, dass jede konkrete Beschreibung eines Systems Ergebnis einer bestimmten Betrachtungsweise ist. Es gibt daher keine allgemein gültige Beschreibung eines Systems, aus der eine aufgabenbezogene Systembeschreibung nach einfachen Regeln abgeleitet werden könnte. Die Gewinnung einer für die Systemanalyse geeigneten Beschreibung ist selbst ein analytischer Vorgang. Dabei sind teilweise konkurrierende Anforderungen zu stellen:

- „Die Systembeschreibung muss so einfach wie möglich sein, um die Übersichtlichkeit zu erhalten und den Aufwand zu begrenzen.
- Sie muss so vollständig sein, dass sie die für die Fragestellung wichtigen Komponenten und deren Beziehungen enthält, da andernfalls die Ziele der Analyse nicht erreicht werden können.
- Die Beschreibung muss bei umfangreichen Systemen so sein, dass über die Definition geeigneter Schnittstellen eine Gliederung in Teilsysteme möglich ist, die getrennt einer Untersuchung unterzogen werden können“ (/85/, Seite 33).

Nach den einzuhaltenden Vorgaben aus der zukünftigen Gesetzgebung (CSM-Recommendation) sowie den genannten allgemeinen Anforderungen sollte eine angemessene Systembeschreibung also die folgenden Eigenschaften besitzen (siehe Tabelle 4-1):

Tabelle 4-1 Anforderungen an eine Systembeschreibung

| <u>Definition (was?)</u> | <u>Beschreibung (wie?)</u> |
|--|--|
| <ul style="list-style-type: none">• Zielsetzung• Systemfunktionen• Systemgrenzen• Schnittstellen• Systemumgebung | <ul style="list-style-type: none">• Generisch• Einfach• Vollständig• Widerspruchsfrei• Angemessene Systemebene |

Es gibt eine Vielzahl an Beschreibungsmitteln, Methoden und Werkzeugen für eine Systemdefinition. Einige werden z. B. in der EN 50128 (/29/) genannt. Bislang ist es zumindest in der Eisenbahntechnik jedoch nicht gelungen, sich auf einen einzigen Ansatz zu einigen. Auch eine geplante allgemeine funktionale Beschreibung des Eisenbahnsystems, das in der CENELEC Norm EN 50127 (Railway Applications – guide to the specification of a guided transport system) realisiert werden sollte, scheiterte.

Die Praxis hat gezeigt, dass Experten die Erstellung einer Systemdefinition immer wieder unterschätzen und dass trotz erheblichen Aufwandes und hoher Kosten auch immer wieder Systeme versagen, weil die Systemdefinition fehlerhaft oder zumindest interpretierbar war. Nach /9/ (Seite 31) kann man allerdings feststellen, dass allein die intensive Beschäftigung mit dem Thema Systemdefinition einen Nutzen bringt, unabhängig davon, welches Beschreibungsmittel schließlich gewählt wird.

Die Definition eines Systems ist der Schlüssel zu den im Analyseprozess folgenden Schritten. Denn „ohne eine präzise Systemdefinition kann die gesamte Analyse zu falschen oder ungültigen Ergebnissen führen. Dies hat sich auch in der Praxis darin gezeigt, dass typischerweise der Anteil des Aufwands für die Systemdefinition in realen Risikoanalysen unterschätzt wurde und nach Beendigung festgestellt werden musste, dass gerade der Aufwand für die Systemdefinition einen erheblichen Anteil am Gesamtbudget ausmachte“ (/9/, S. 31).

4.2 Systemdefinition

Das System, das mit BP-Risk betrachtet werden soll, erbringt seine Funktion durch das Zusammenwirken von Mensch und Technik (siehe Abbildung 4-2).

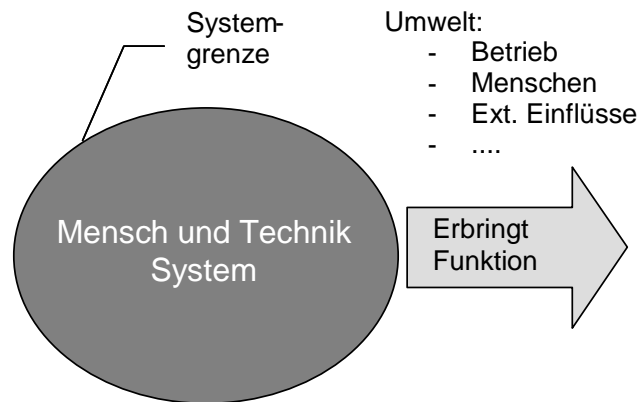


Abbildung 4-2 Prinzip der Systemdefinition für BP-Risk (nach /9/)

Im konkreten Fall ist das System, was BP-Risk betrachtet, ein Zug mit der Betrachtungseinheit ‚eine Stunde Zugfahrt‘. Zur Identifizierung von gültigen Funktionen für dieses System steht im Anhang eine Funktionsliste aus der Schienenfahrzeugtechnik zur Verfügung, die auf einer für das Risikomodell von BP-Risk abgestimmten Systemebene definiert ist (siehe Anhang E: Funktionsliste). Die Erarbeitung dieser Funktionsliste als Systemdefinition wird in den folgenden Kapiteln näher erläutert.

4.2.1 prEN0015380-4

Die Grundlage der Funktionen für das Teilsystem Fahrzeug bildet die TSI RST (Technical Specification for Interoperability¹⁵ – Rolling Stock). Sie bilden den Ausgangspunkt für die Funktionsgruppen für Schienenfahrzeuge der europäischen Vornorm prEN 0015380 (Teil 4). Die Funktionen der prEN 0015380 bilden wiederum die Basis der Systemdefinition für BP-Risk.

Der Normentwurf prEN 0015380-4 (Stand Juni 2007) deckt die Anforderungen der TSI des Teilsystems Fahrzeuge und die Anforderungen aus dem CENELEC Technical Report TR 50126-3 (/31/) ab und ergänzt diese Regelwerte. Als Grundlage für die prEN 0015380-4 dienten die DIN 25002 Teil 5 (Entwurf) sowie die MODTrain Struktur der UNIFE¹⁶, die der AEIF¹⁷ Struktur entspricht (siehe auch Abbildung 4-3).

¹⁵ Die Technischen Spezifikationen für die Interoperabilität (TSI) werden im Anhang C: TSI erläutert.

¹⁶ UNIFE : Union des Industries Ferroviaires Européennes (Europäischer Verband der Bahnindustrie)

¹⁷ AEIF: Association Européenne pour l'Interopérabilité Ferroviaire (Europäische Vereinigung für die Interoperabilität im Bereich der Bahn).



Abbildung 4-3 MODTrain Struktur (aus dem Englischen nach /94/)

Die Funktionsgruppen der prEN 0015380-4 beschreiben die im Fahrzeug zu realisierenden Funktionen, ungeachtet ihrer fahrzeugspezifischen technischen Umsetzung. Dabei folgt die prEN 0015380-4 der IEC 61226, die eine Funktion definiert als: „*bestimmter Zweck oder zu erreichendes Ziel, das spezifiziert oder näher beschrieben werden kann, ohne Bezug auf die physikalischen Mittel zu nehmen*“ (aus dem Englischen nach /75/).

Bei der Benennung der Funktionen wurde daher darauf geachtet, dass die grundsätzlichen Überlegungen eingehalten werden, Funktionen als solche auszudrücken und nicht stattdessen auf die Benennung von Funktionsträgern auszuweichen. Die beispielhafte Zuordnung bekannter Funktionsträger im Rahmen der Norm dient der Verdeutlichung. Dabei ist zu beachten, dass durch die Vorgabe der Betrachtung eines Schienenfahrzeugs natürlich eine gewisse ‚Realisierung‘ von Funktionen vorgegeben ist. So soll bei der Funktionsbeschreibung insbesondere nicht die interne Implementierung innerhalb des Schienenfahrzeugs betrachtet werden. Es soll freigestellt sein, ob die Funktion ‚Bremsen‘ manuell durch den Menschen erfolgt, indem er einen Bremshebel betätigt, oder automatisch durch eine elektronische Ansteuerung. Dass ein Schienenfahrzeug jedoch grundsätzlich Bremsen besitzt, um die Geschwindigkeit zu reduzieren und um zum Stehen zu kommen, wird vorausgesetzt und nicht als ‚technische Realisierung‘ angesehen. Dazu sagt die DIN 25002-5: „*Zwischen einer Funktion und ihrer technischen Realisierung besteht nicht zwangsläufig ein eindeutig umkehrbarer Zusammenhang. Eine Betrachtungseinheit¹⁸ kann gleichzeitig oder sequentiell Funktionsträger für mehrere Funktionen sein. Das bedeutet, dass einer Betrachtungseinheit bei der Strukturierung durchaus mehrere Funktionen zugewiesen werden können*“ (/43/, Seite 4).

¹⁸ Teil, Bauelement, Gerät, Teilsystem, Funktionseinheit, Betriebsmittel oder System, das für sich allein betrachtet werden kann (/43/, Seite 4).

Die Hauptfunktionen der prEN 0015380-4 entsprechen fast komplett den Hauptfunktionen der DIN 25002 Teil 5 (10 Hauptfunktionen¹⁹) und lauten:

1. „Transportgut tragen, umschließen, schützen,
2. Aufenthalts-, Arbeits- und Transportbedingungen sicherstellen,
3. Zugang und Beladen sicherstellen,
4. Fahrzeuge verbinden,
5. Hilfsenergie und Medien bereitstellen,
6. Fahren und Bremsen,
7. Fahrzeug übergeordnet leiten,
8. Spurführung und Laufgüte sicherstellen,
9. Fahrzeug in das Gesamtsystem Bahn integrieren“ (aus dem Englischen /32/, S. 13).

Die Kennzeichnung der Funktionen in der prEN 0015380-4 erfolgt mit den Buchstaben des Alphabets, jedoch nicht die Verwendung der Buchstaben I und O sowie Sonderzeichen und Trennzeichen. Die Haupt- und Teilfunktionen werden in ihrer jeweiligen Ebene einstellig codiert (siehe Tabelle 4-2 für einige Beispiele). Die Kennzeichnung beginnt mit der Angabe der Hauptfunktion und wird um die Kennzeichnung der Teilfunktionen bis maximal zur 5. Ebene fortgesetzt, wobei die Ebenen vier und fünf im informativen Anhang der prEN 0015380-4 aufgezählt werden.

Bei der Nennung des Beispiels in Tabelle 4-2 sei erwähnt, dass die prEN 0015380-4 nur in englischer Sprache verfasst ist, wobei es noch keine offizielle deutsche Übersetzung gibt. Der deutsche Vorgänger, die DIN 25002-5, kann nur teilweise als Übersetzung herangezogen werden, da beispielsweise die DIN nur drei Funktionsebenen und die prEN 0015380-4 fünf Ebenen beschreibt. Deswegen werden die englischen Beispiele aus der Norm und dort wo es Parallelen zur DIN gibt, die deutsche Fassung angegeben.

Tabelle 4-2 Funktionen der prEN0015380-4 (Beispiele)

| Level | | | | | Function (level 1 to 5) | example / explanation |
|-------|---|---|---|---|--|--|
| 1 | 2 | 3 | 4 | 5 | | |
| B | | | | | Carry and protect passengers, train crew and payload | Ride comfort not considered |
| B | B | | | | Arrange interior space | Interior design |
| B | B | B | | | Provide floor and flooring | Non slip floor covering |
| B | B | C | | | Provide roof and roofing | |
| B | E | D | | | Manage signaling of fire | Management of fire alert, fire warning, notification of fire |
| B | E | E | * | | Manage/Prove-fire extinguishment | |
| B | E | E | * | B | Manage automatical fire extinguish system | |
| B | E | E | * | C | Monitor volume of extinguishing agent | |
| B | E | E | * | D | Provide manual fire extinguish facilities | |

¹⁹ In der DIN wurden die Funktionen ‚Fahren‘ und ‚Bremsen‘ noch unterschieden (/43/).

Die Unterscheidung der Ebenen wird in der Norm lediglich verbal beschrieben:

- „*Funktionsebene: Hierarchieebene, um Funktionen mit dem gleichen Zweck zusammenzufassen;*
- *Erste Funktionsebene (Hauptfunktion): Funktion der Betrachtungseinheit Schienenfahrzeug auf oberster Ebene (Ebene 1).*
- *Zweite Funktionsebene (Teilfunktion): Teilaspekt einer Hauptfunktion (Ebene 2). Auf dieser Ebene wird NICHT besagt, wie die Funktion implementiert wird. Eine spezifische Funktion auf zweiter Ebene betrifft in der Regel eine Ingenieurs-Disziplin und kann von einem oder einer minimalen Anzahl von Subsystemen unterstützt werden.*
- *Dritte Funktionsebene (Unterfunktion): Teilaspekt einer Teilfunktion (Ebene 3). Eine Funktion auf dieser Ebene sollte so weit wie möglich von einem einzigen Subsystem unterstützt werden“ (/43/ und /32/, Seite 6ff).*

In der Norm werden auch so genannte „*Transverse Functions*“ (Querfunktionen) definiert. Diese Funktionen betreffen zum größten Teil die Ebenen zwei und drei der FBS („*Functional Breakdown Structure*“) gleichzeitig. Deswegen werden sie in der FBS nicht als Subfunktionen eingefügt, sondern in einer gesonderten Tabelle beschrieben (siehe Tabelle 4-3). Diese Querfunktionen werden im Rahmen der Systemdefinition von BP-Risk vorerst nicht weiter berücksichtigt.

Tabelle 4-3 Transverse Functions (Beispiele)

| Level | | | Transverse function | description / remark |
|-------|---|---|-------------------------------------|--|
| 1 | 2 | 3 | | |
| V | | | Provide control | used for a function to describe the man machine interface for the control command related function |
| Z | | | Communicate with ground level | used for a function to provide list of information to forward and receive from the ground related function |
| Z | A | | Transmit information to the ground | used for a function to provide list of information to forward to the ground related function |
| Z | B | | Receive information from the ground | used for a function to provide list of information to be received from the ground related function |

4.2.2 Anpassung für BP-Risk

Ein wichtiger Aspekt für die Anwendbarkeit von BP-Risk ist die zu betrachtende Systemebene. BP-Risk ist auf einer festgelegten Ebene kalibriert (siehe Kapitel 7) und ist nur auf dieser Ebene gültig und anwendbar. Eine Anwendung von BP-Risk auf einer anderen als die Kalibrierungsebene würde zu falschen Ergebnissen führen.

Um eine Systemdefinition für BP-Risk zu erstellen, ist es also wichtig, eine eindeutige Betrachtungsebene festzulegen. Die Systemdefinition aus der Kalibrierung nach 7.2.1 entspricht dem Systemlevel eines fahrzeugseitigen Zugbeeinflussungs-Systems im Hochgeschwindigkeitsverkehr. Die entsprechenden Funktionen der prEN 0015380-4 befinden sich auf zweiter und dritter Funktionsebene und lauten (siehe Tabelle 4-4):

Tabelle 4-4 Funktionsgruppe Zugbeeinflussung

| Ebene | | | Funktion | Beispiel/Erläuterung (aus DIN 25002-5) |
|-------|---|---|--|---|
| 1 | 2 | 3 | | |
| K | E | | Automatische Zugsicherung/-steuerung bereitstellen | Fahrerloses Fahren gewährleisten |
| K | E | B | ATC-Schnittstelle bereitstellen | über ATC in das Gesamtsystem integrieren |

Somit werden zur Festlegung der Systemdefinition die Funktionen der prEN 0015380-4 betrachtet, die der zweiten *und* dritten Ebene entsprechen. Bei der Auswahl der Funktionen wurde darauf geachtet, eine hohe Systemebene festzulegen, da

- der Risikozielwert aus der Kalibrierung auf die gesamte (fahrzeugseitige) Zugbeeinflussung bezogen wird,
- nicht die technische Realisierung der Funktionen festgelegt werden soll, und
- der BP-Risk Ansatz eine hohe Systemebene als Input fordert (siehe Kapitel 5.3).

Die Funktionen der zweiten und dritten Ebene bilden somit die Grundlage für eine generische Systemdefinition, da die Norm prEN 0015380-4 die oben genannten Anforderungen an eine Systemdefinition erfüllt (siehe Tabelle 4-5).

Tabelle 4-5 Anforderungen an Systemdefinition

| Anforderungen | prEN 0015380-4 |
|----------------------|--|
| Zielsetzung | Grundlage einer generischen Systemdefinition für BP-Risk |
| Systemfunktionen | Fahrzeugfunktionen |
| Systemgrenzen | Schienenfahrzeug |
| Schnittstellen | Schnittstellenbeschreibung möglich |
| Systemumgebung | Streckenfunktionen u. a. |
| Generik | Funktionen unabhängig von ihrer technischen Realisierung |
| Einfachheit | Strukturiert in Ebenen, Beschreibung mit Beispielen |
| Vollständigkeit | Annahme der Vollständigkeit aufgrund der Normung |
| Widerspruchsfreiheit | Annahme der Widerspruchsfreiheit |
| Systemebene | Angemessene Ebene wählbar |

Die Zielsetzung der Systemdefinition besteht darin, einen Ausgangspunkt für eine korrekte BP-Risk Analyse zu liefern und somit dem Anwender eine Hilfestellung zu geben, so dass er BP-Risk auf der richtigen Ebene anwendet. Die prEN 0015380-4 bildet die Grundlage einer generischen Systemdefinition, da die Fahrzeugfunktionen unabhängig von ihrer technischen Realisierung beschrieben werden.

Es wird angenommen, dass die Norm vollständig und widerspruchsfrei ist. Widersprüchlich im Rahmen einer funktionalen Systemdefinition wäre beispielsweise der Fall, wenn sich Funktionen überlappen oder sich Funktionen bei ihrer Ausführung gegenseitig ausschließen.

Ob dies bei der prEN 0015380-4 der Fall ist, kann schwer nachgeprüft werden, da es sich um generische Funktionen handelt. Ohne die technische Realisierung und ohne die Zuweisung von Komponenten sind eventuelle Überlappungen oder Ausschlüsse nicht feststellbar. Die obigen Annahmen können jedoch damit begründet werden, dass eine Norm auf dem Weg zur Veröffentlichung viele Durchsichten und Reviews überstehen muss und somit von zahlreichen Experten geprüft wird, so dass von Vollständigkeit und Widerspruchsfreiheit ausgegangen werden kann.

Die Vorgabe der Betrachtungsebene für BP-Risk durch die Kalibrierung kann in der Systemdefinition berücksichtigt werden, da die prEN 0015380 in Ebenen strukturiert ist. Die vorgegebene Funktion der Kalibrierung findet sich in der Norm wieder und definiert somit die für BP-Risk angemessene Systemebene.

Das betrachtete System wird in der Norm prEN 0015380-4 durch Fahrzeugfunktionen beschrieben. Damit wird das System eindeutig abgegrenzt und es ist eine Schnittstellenbeschreibung an der Systemgrenze möglich. Diese wird im folgenden Kapitel 4.2.3 zur Identifizierung von zusätzlichen Funktionen aus der Systemumgebung genutzt.

4.2.3 Zusätzliche Funktionen

Es wird davon ausgegangen, dass die Funktionsgruppen der prEN 0015380-4 vollständig die Funktionen für ein Schienenfahrzeug beschreiben. Die Grundidee bei der generischen Systemdefinition mit Hilfe der prEN 0015380-4 besteht nun darin, dass ausgehend von einer vollständigen Beschreibung der Fahrzeugfunktionen und zusätzlich einer vollständigen Schnittstellenbeschreibung alle Funktionen und somit auch Gefährdungen für das Eisenbahnsystem auf der für BP-Risk korrekten Ebene ermittelt werden können.

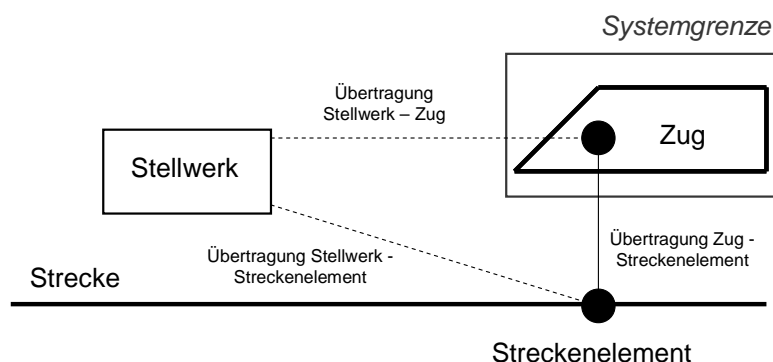


Abbildung 4-4 Systemdefinition BP-Risk

BP-Risk definiert als Betrachtungsgegenstand einen Zug. Abbildung 4-4 zeigt dafür die Systemgrenze und beispielhaft die Schnittstellen zur Leit- und Sicherungstechnik. An den Schnittstellen werden nun ‚zusätzliche‘ Funktionen identifiziert durch die Betrachtung einer Zugfahrt. Es werden diejenigen Funktionen an den Schnittstellen beschrieben, denen ein Schienenfahrzeug auf seiner Fahrt begegnet, siehe Tabelle 4-6 für einige Beispiele.

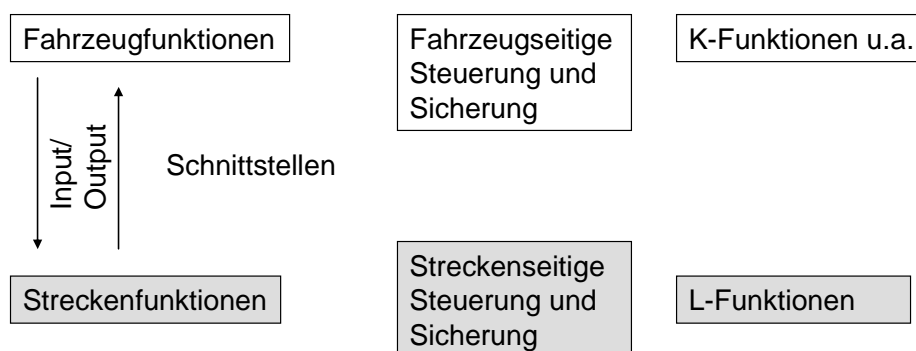
Tabelle 4-6 Beispiele für zusätzliche Funktionen

| Ebene | | | Funktion | Erläuterung |
|-------|---|---|----------------------------------|-----------------------------------|
| 1 | 2 | 3 | | |
| K | D | B | Signaltechnische Beeinflussung | Funktionsgruppe aus prEN0015380-4 |
| L | B | D | Streckenseitige Zugbeeinflussung | Zusätzliche Streckenfunktion |
| K | G | B | Streckenführung wählen | Funktionsgruppe aus prEN0015380-4 |
| L | B | F | Bewegl. Fahrwegelemente sichern | Zusätzliche Streckenfunktion |
| K | G | C | Signale steuern und überwachen | Funktionsgruppe aus prEN0015380-4 |
| L | B | G | BÜ sichern | Zusätzliche Streckenfunktion |

Dabei werden vorerst nur diejenigen Streckenfunktionen betrachtet, die sich an der Schnittstelle ‚Zug-Streckenelement‘ befinden. Die Schnittstelle ‚Stellwerk-Zug‘ wird erst einmal nicht betrachtet, da es sich dort in der Regel um eine zentrale Ansteuerung per Funk, z. B. ausgehend von einer Streckenzentrale, (Radio Block Center, RBC) handelt. Diese zentralen Funktionen werden in Kapitel 8 im Rahmen der Umrechnung gesondert berücksichtigt.

Bei der Betrachtung der Schnittstellen und der Identifizierung von zusätzlichen Funktionen wird deutlich, dass eine vollständige Funktionsliste für das *gesamte* Eisenbahnsystem den Rahmen dieser Arbeit sprengen würde, da es nicht Ziel dieses Dissertationsprojektes ist, eine generische Beschreibung des gesamten Eisenbahnsystems zu liefern. Die Funktionsliste soll lediglich dem Anwender helfen, die richtige Ebene für BP-Risk zu betrachten. So liegt der Fokus der vorliegenden Arbeit darauf, insbesondere die Schnittstellen zur Leit- und Sicherungstechnik zu untersuchen und für diesen Bereich die zusätzlichen Funktionen zu identifizieren. Die nicht betrachteten Bereiche, wie z. B. Elektrifizierung, bleiben Bestandteil weiterer Forschungsarbeiten.

Die Funktionsliste inklusive der zusätzlichen Funktionen für den Bereich Leit- und Sicherungstechnik befindet sich im Anhang dieser Arbeit (siehe Anhang E: Funktionsliste). Dabei wurde für die zusätzlichen Funktionen der Codebuchstabe *L* eingeführt. Dieser kennzeichnet alle Streckenfunktionen, die an den Fahrzeugschnittstellen beschrieben wurden (siehe Abbildung 4-5). Die zugeordneten Schnittstellen der Fahrzeugfunktionen aus der Norm sind in einer gesonderten Spalte (Interface / Schnittstelle) vermerkt.

**Abbildung 4-5 Schnittstellenbeschreibung**

Wenn man den ERA-Prozess aus Kapitel 2.1.2 (siehe Abbildung 2-2) zugrunde legt, folgt auf Basis der erarbeiteten Systembeschreibung die Identifikation der Gefährdungen, die sich aus einem Versagen einer Funktion ergeben. Diese Gefährdungen sind im weiteren Vorgehen die Eingangsdaten für die anschließende Risikobewertung (mit Hilfe von BP-Risk).

4.3 Gefährdungsidentifikation aus der Funktionsliste

Eine Gefährdung ist nach CENELEC „ein Objekt, eine Bedingung oder ein Zustand, der zu einem Unfall führen kann“ (/30/). Im Zusammenhang mit der Systemsicherheit ist eine Gefährdung ein ungesicherter Zustand des Systems, der unter bestimmten äußeren Bedingungen zu einem Unfall führt. Die Identifikation der betrieblichen Gefährdungen erfolgt im Bezug auf die Systemgrenze (Schienenfahrzeug) und bildet den Ausgangspunkt für die Folgen- und Schadensanalyse mit Hilfe von BP-Risk.

Im Allgemeinen beinhaltet die Gefährdungsidentifikation eine systematische Analyse des Systems und umfasst zwei Phasen:

- „eine empirische Phase (Nutzung von in der Vergangenheit gemachten Erfahrungen, z. B. Checklisten oder Lehren aus Beinahe-Unfällen) und
- eine kreative Phase (Vorhersagen, z.B. strukturierte „Was-wäre-wenn-Studien“ in Art einer FMEA²⁰)“ (/9/, Seite 32).

Die empirische und die kreative Phase der Gefährdungsidentifikation ergänzen einander, so dass man darauf vertrauen kann, dass der potenzielle Gefährdungsraum abgedeckt ist und alle signifikanten Gefährdungen identifiziert werden. Für die empirische Phase können Gefährdungen aus bereits vorhanden (empirischen) Gefährdungslisten in Betracht gezogen und ggf. ergänzt und oder angepasst werden. Im Rahmen der kreativen Phase kann eine vereinfachte funktionale FMEA für die identifizierten Funktionen aus der Systemdefinition (Funktionsliste) durchgeführt werden. Das hier zu Grunde liegende Gefährdungsmodell ist in Abbildung 4-6 dargestellt.

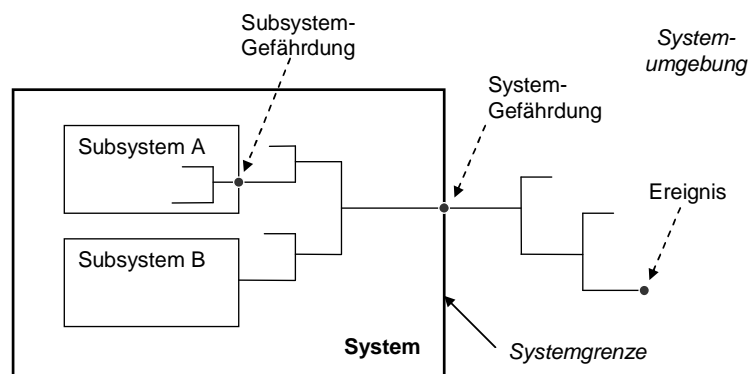


Abbildung 4-6 Gefährdungsmodell

²⁰ FMEA: Failure Mode and Effects Analysis

Dabei soll noch einmal erwähnt werden, dass die Gefährdungen immer an der Systemgrenze definiert werden. Abbildung 4-6 macht deutlich, dass eine Subsystem-Gefährdung an der Systemgrenze von Subsystem A eine Gefährdung sein kann, wenn man nur das Subsystem A betrachten würde. Wenn die Betrachtung jedoch vom gesamten System ausgeht, so ist die Subsystemgefahr von Subsystem A lediglich eine Ursache für die Systemgefahr an der Systemgrenze des gesamten Systems.

Eine generische Gefährdungsidentifikation ist auf Basis der erstellten Funktionsliste für ein Schienenfahrzeug möglich. Dazu kann für eine grobe Abschätzung *„aus der Liste der Systemfunktionen durch Negation eine Liste der Systemgefahren abgeleitet werden. Dieses Ergebnis sollte durch eine Schnittstellen - FMEA abgesichert werden“* (/9/, Seite 99).

Die *„Failure Mode and Effects Analysis“* (FMEA) ist eine Methode zur systematischen Vorgehensweise, um potenzielle Schwachstellen zu finden. Sie wird beschrieben in der IEC 60812 (/77/). Im engeren Sinne ist die FMEA beschränkt auf eine qualitative Analyse der Ausfallmodi von Hardwarekomponenten. Sie schließt eigentlich keine menschlichen Fehler oder Softwarefehler ein, obwohl gegenwärtige Systeme diesen in der Regel ausgesetzt sind. Im weitesten Sinne können solche Faktoren jedoch mit betrachtet werden, was die ERA zur Identifizierung von Gefährdungen auch fordert: menschliche Faktoren, Umweltbedingungen und alle Betriebsmodi sollen berücksichtigt werden (siehe /59/, Artikel 7). Nach IEC 60812 beinhaltet eine FMEA u. a. folgende Schritte:

1. System abgrenzen,
2. Systemfunktionen beschreiben,
3. Versagensmodi festlegen,
4. Analyse durchführen.

Im Folgenden wird beispielhaft eine Gefährdungsbetrachtung anhand einer vereinfachten funktionalen FMEA für einen Bahnübergang (BÜ) vorgestellt.

4.3.1 Beispiel: BÜ

1.) System abgrenzen

Das System ist abgegrenzt durch die vorgegebene Funktionsliste der prEN 150380 mit zusätzlichen Funktionen an den Schnittstellen zur Leit- und Sicherungstechnik. In Anlehnung an die Systemdefinition im vorigen Kapitel zeigt Abbildung 4-7 die Systemgrenzen und die zugehörige Schnittstelle. Es wird davon ausgegangen, dass die Bahnübergangssicherungsanlage (BÜSA) vom Fahrzeug aktiviert wird (d. h. das Fahrzeug wird von der BÜSA detektiert), so dass in diesem Fall das Stellwerk keine Rolle spielt.

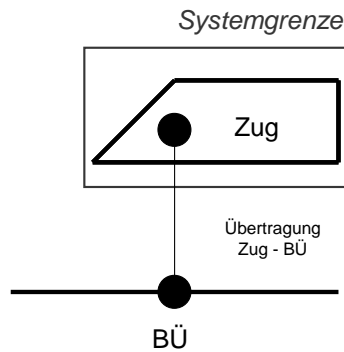


Abbildung 4-7 Schnittstelle Zug - BÜ

2.) Systemfunktionen beschreiben

Die zu betrachtende Systemfunktion laut Funktionsliste (Funktion LH) heißt: „*BÜ sichern*“. Diese befindet sich an der Schnittstelle zwischen Zug und BÜ. Es wird im Rahmen dieses Beispiels von einer zuggesteuerten Anlage ausgegangen. Die Sicherung für den Straßenverkehr (in Form von Lichtzeichen- oder Blinklichtanlagen mit oder ohne Halbschranken) werden vom Zug über Einschaltkontakte im Gleis eingeschaltet und über Ausschaltkontakte oder eine Induktionsschleifen ausgeschaltet. Bei der Überwachung wird i. d. R. unterschieden zwischen dem Überwachen der eingetretenen Sicherung (Hp^{21} und $ÜS^{22}$) und dem Überwachen der Verfügbarkeit der Anlage ($Fü^{23}$ und $ÜS_{oE}^{24}$). Dadurch ergeben sich verschiedenen Informationsinhalte an den Schnittstellen BÜSA – Stellwerk oder Überwachungssignal (BÜSA) – Tf. Für das vorliegende Beispiel wird zur Vereinfachung nur die Überwachungsart ÜS betrachtet.

Bei der Überwachungsart ÜS signalisieren sogenannte Überwachungssignale dem Triebfahrzeugführer, dass die BÜSA eingeschaltet wurde und ordnungsgemäß arbeitet. Die Überwachungssignale sind im Bremswegabstand vor dem BÜ aufgestellt, so dass der Zug bei Versagen der Einschaltung vor dem BÜ anhalten kann. Falls das ÜS anzeigt, dass die Sicherungsanlage nicht eingeschaltet wurde, muss der BÜ manuell gesichert werden. Das Schienenfahrzeug muss vor der Straße anhalten und anschließend muss der BÜ behelfsmäßig oder örtlich gesichert werden. Das Befahren des BÜs ist dann nur mit größter Vorsicht und unter Abgabe akustischer Achtungssignale zulässig. *„Wegen der allgemein guten Sichtbarkeit der Schienenfahrzeuge darf aber wieder beschleunigt werden, sobald die Zugspitze die Straße gequert hat“* (/66/, Seite 399).

Die Ausschaltung erfolgt durch verschiedene lineare Systeme, z. B. Achszählkreise oder Schaltpunkte. Die BÜSA wird ausgeschaltet, sobald der Zug den betreffenden Abschnitt geräumt hat (wenn der BÜ ‚frei‘ gefahren ist).

²¹ Hp: Hauptsignal.

²² ÜS: Überwachungssignal.

²³ Fü: Fernüberwacht.

²⁴ ÜS_{oE}: Überwachungssignal mit optimierter Einschaltung.

3.) Versagensmodi festlegen

Da der Betrachtungsgegenstand ein Schienenfahrzeug ist, sind nur diejenigen Gefährdungen relevant, die auf den Zug wirken. Das bedeutet, es werden nur diejenigen Funktionsversagen betrachtet, die für einen Zug gefährlich werden und zu einem Unfall führen können, z. B. die Kollision eines Zuges am BÜ mit einem Hindernis (Straßenfahrzeug, Fußgänger oder liegengebliebenes Hindernis). Unfälle, die den BÜ allein betreffen, wie z. B. die Kollision eines Verkehrsteilnehmers mit einer Schranke, werden nicht betrachtet.

Für die grobe Abschätzung lautet die Gefährdung aus der Negation der Funktion: *„BÜ nicht gesichert“*. Bei einer ergänzenden Durchführung einer funktionalen FMEA werden die verschiedenen Ausfallmodi der Funktion betrachtet. Die IEC 60812 (/77/) beschreibt die allgemeinen Versagensmodi wie folgt:

- Funktion wird nicht ausgeführt (totaler Ausfall),
- Funktion wird nicht zur vorgeschriebenen Zeit ausgeführt,
- Funktion wird nicht zur vorgeschriebenen Zeit beendet,
- Funktion wird vorzeitig ausgeführt.

Angewendet auf die Beispielfunktion, lauten die Versagensmodi:

- a) BÜ-Sicherung wird nicht ausgeführt (totaler Ausfall),
- b) BÜ-Sicherung wird nicht zur vorgeschriebenen Zeit ausgeführt,
- c) BÜ-Sicherung wird nicht zur vorgeschriebenen Zeit beendet,
- d) BÜ-Sicherung wird vorzeitig ausgeführt.

4.) Analyse durchführen

Bei der Betrachtung der Versagensmodi ist es wichtig, sie in einen betrieblichen Kontext zu setzen. Was bedeutet also ein totaler Ausfall der BÜ-Sicherung betrieblich? Dazu muss auch bekannt sein, wie die BÜ-Sicherung funktioniert.

Fall a)

Ein mögliches Szenario für den ersten Fall wäre zum Beispiel, dass sowohl die straßenseitige Sicherung (Lichtzeichen), als auch die schienenseitige Sicherung (Überwachungssignal) versagt. Dabei ist es wichtig zu unterscheiden, ob ein Ausfallmodus wirklich gefährlich ist (also zu einem Unfall führen könnte) oder nur betriebshemmend wirkt. Dazu müssen die betrieblichen Auswirkungen des Funktionsausfalls betrachtet werden.

Beim Bahnübergang gibt es beispielsweise folgenden Auswirkungen:

- BÜ steht unerkannt ungesichert offen (gefährlich).
- BÜ ist nach Fehler dauerhaft geschlossen (betriebshemmend).

In beiden Fällen ist die Sicherungsanlage ‚ausgefallen‘. Der zweite Ausfallmodus ist vorerst nur betriebshemmend, da der BÜ trotzdem durch die geschlossenen Schranken gesichert ist. Jedoch kann solch eine Situation auch gefährlich werden, da möglicherweise die wartenden Straßenverkehrsteilnehmer ungeduldig werden und bei langem nicht Erscheinen eines Zuges die BÜ-Sicherung umgehen. In einem solchen Fall sind also die menschlichen Handlungen ausschlaggebend, ob es zu einer Gefährdung kommt oder nicht (siehe dazu /58/).

Laut DB AG Statistiken (/38/) sind 98 Prozent der Unfälle an Bahnübergängen auf das Fehlverhalten der Straßenverkehrsteilnehmer zurückzuführen (siehe Abbildung 4-8). Leichtsinn, Unaufmerksamkeit oder Unkenntnis sind in den meisten Fällen die Ursache.

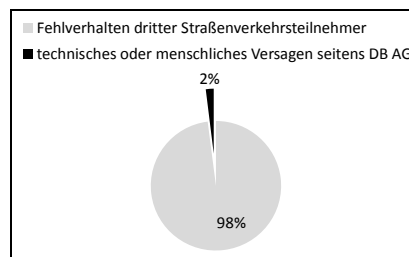


Abbildung 4-8: Unfallursachen an Bahnübergängen (nach /38/)

Fall b)

Wird die BÜ-Sicherung nicht zur vorgeschriebenen Zeit ausgeführt, kann dies auch bezeichnet werden als ‚Sicherung zur Unzeit‘, z. B. das Schließen der Schranken zur Unzeit. Zu erwähnen ist hierbei, dass der BÜ als gesichert gilt, wenn die Rotlichter das erste Mal aufleuchten. *„Grundvoraussetzung dafür, dass ein mit einer BÜSA ausgerüsteter BÜ als ‚ordnungsgemäß gesichert‘ gilt, ist bei Bahnübergängen mit optischen Signalgebern das Leuchten aller dieser Siganlageber mit rotem Blink-oder Dauerlicht, unabhängig davon, ob zusätzlich Voll- bzw. Halbschrankenbäume vorhanden sind“* (/66/, Seite 394).

Beim Schließen der Schranken zur Unzeit kann ein Verkehrsteilnehmer ohne Vorwarnung gegen die Schranken fahren. Laut Continentalstudie ist *„jeder sechste Autofahrer zumindest in Ausnahmefällen bereit einen Bahnübergang trotz sich senkender Schranken zu queren“* (/58/, Seite 214). Dieses wäre ein Unfalltyp, der nicht den Zug betrifft und insofern nicht weiter betrachtet wird.

Fall c)

Wird die BÜ-Sicherung nicht zur vorgeschriebenen Zeit beendet, würde dies im vorliegenden Beispiel besagen, dass die Ausschaltung vorzeitig erfolgt. Dies bedeutet betrieblich, dass der Zug sich noch im Kreuzungsbereich mit der Straße befindet und die Schranken bereits geöffnet werden. Dieses Szenario wäre nur dann gefährlich, wenn der Zug das Überwachungssignal schon passiert hat, aber noch nicht am BÜ angekommen ist. Allerdings ist hierbei zu beachten, dass es bereits Unfälle gab, wo Verkehrsteilnehmer in den fahrenden Zug gefahren sind (siehe /99/ und /100/).

Ein anderer Fall für die nicht rechtzeitige Beendigung der Sicherung wäre z. B., dass die roten Lichtzeichen eingeschaltet bleiben bzw. die Schranken sich nicht öffnen, obwohl der Zug den BÜ geräumt hat. Diese Situation könnte die Straßenverkehrsteilnehmer dazu verleiten, die Warneinrichtungen zu ignorieren. Laut Continentalstudie ist „fast jeder Fünfte bereit, zumindest in Ausnahmefällen Halbschranken zu umgehen oder zu umfahren“ (/58/, Seite 214).

Fall d)

Wird die BÜ-Sicherung vorzeitig ausgeführt, würde das für den Beispielfall einer zu frühen Sicherung entsprechen. Eine zu frühe Einschaltung wäre betrieblich allerdings nicht gefährlich, sondern nur betriebshemmend. Die Straßenverkehrsteilnehmer müssten jedoch länger am BÜ warten, was wiederum zu Ungeduld führen kann. „Nach mehr als 15 Minuten Wartezeit lassen 40% der Autofahrer eine gewissen Bereitschaft erkennen, ein rotes Lichtsignal zu missachten, und bei Fußgängern und Radfahrern sind sogar mehr als die Hälfte hierzu bereit“ (/58/, Seite 215).

Tabelle 4-7 Zusammenfassung funktionale FMEA

| | Ausfallart | Beispiel | Folge | Gefährdung |
|---|---|---|---|---|
| a | BÜ-Sicherung wird nicht ausgeführt (totaler Ausfall). | Überwachungssignal zeigt BÜ ist gesichert obwohl BÜ nicht gesichert ist. Lichtzeichen bleibt dunkel, obwohl es rot zeigen sollte; Schranken werden nicht geschlossen, obwohl Zug sich nähert. | Schienenfahrzeug überfährt ungesicherten BÜ. | ja |
| b | BÜ-Sicherung wird nicht zur vorgeschriebenen Zeit ausgeführt. | Schließen der Schranken zur Unzeit; Einschaltung der Lichtsignale zur Unzeit. | 1) Straßenverkehrsteilnehmer fährt gegen Schranke; 2) Schienenfahrzeug befährt ungesicherten BÜ; 3) Schienenfahrzeug trifft zu früh nach eingetretener Sicherung am BÜ ein. | 1) nicht für das Schienenfahrzeug 2) ja 3) ja |
| c | BÜ-Sicherung wird nicht zur vorgeschriebenen Zeit beendet. | 1) BÜSA wird vorzeitig ausgeschaltet; 2) Lichtzeichen bleiben rot oder Schranken werden nicht geöffnet. | 1) Zug überfährt ungesicherten BÜ; 2) Straßenverkehrsteilnehmer wartet, obwohl kein Zug kommt. | 1) ja, wenn Zug ÜS passiert, aber BÜ noch nicht erreicht hat (auch abhängig von menschl. Handlungen) 2) möglich (abhängig von menschl. Handlungen) |
| d | BÜ-Sicherung wird vorzeitig ausgeführt. | BÜ wird vorzeitig eingeschaltet. | Straßenverkehrsteilnehmer wartet, obwohl kein Zug kommt. | möglich (abhängig von menschl. Handlungen) |

Als Ergebnis der FMEA erhält man eine Liste von betrieblichen Gefährdungen der Systemfunktionen, eine Zusammenfassung für das oben genannte Beispiel gibt Tabelle 4-7. Die detaillierte Untersuchung der verschiedenen Ausfallmodi lässt in vielen Fällen den Anwender das System und die Sicherheitsfunktionen besser verstehen, auch wenn möglicherweise keine zusätzlichen Gefährdungen formuliert werden können. Im vorliegenden Beispiel wurden neben dem totalen Ausfall der Sicherung, was der vereinfachten Gefährdung („BÜ nicht gesichert“) entsprechen könnte, auch noch differenziertere Ausfallmodi formuliert, die betrieblich zu einer Gefährdung führen könnten, z. B. die vorzeitige Ein- und Ausschaltung.

4.3.2 Exkurs: Allgemein akzeptierbares Risiko

Laut ERA-Prozess (siehe Abbildung 4-9), soll nach der Gefährdungsidentifikation eine Klassifizierung der Gefährdungen anhand der zugehörigen Risiken erfolgen.

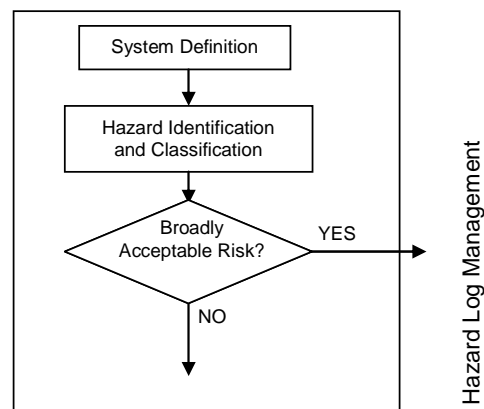


Abbildung 4-9 Allgemein akzeptierbares Risiko (nach /62/)

Gefährdungen mit einem allgemein akzeptierbaren Risiko („*broadly acceptable risk*“) brauchen nicht weiter analysiert zu werden, sondern werden nur im Gefährdungsprotokoll („*Hazard Log*“) eingetragen. Diese Unterscheidung soll laut CSM-Recommendation (/62/) dazu beitragen, den Aufwand einer Risikobeurteilung auf die wichtigsten Risiken zu konzentrieren.

Wie dieser Schritt ganz praktisch durchgeführt werden soll, z. B. anhand einer Klassifizierungsmethode, ist noch unklar. Bislang schreibt die CSM-Recommendation lediglich vor, die Bewertung anhand von Experten und mit Hilfe eines groben qualitativen Kriteriums durchzuführen. Als Kriterium für ‚allgemein akzeptierbare Risiken‘ gibt die CSM-Recommendation an, dass „*Risiken, die von Gefährdungen resultieren, als allgemein akzeptierbar klassifiziert werden können, wenn das Risiko so klein ist, dass es nicht sinnvoll ist, irgendwelche zusätzlichen Sicherheitsmaßnahmen einzuführen*“ (aus dem Englischen nach /62/, Artikel 7). Dabei werden ‚Sicherheitsmaßnahmen‘ definiert als „*Maßnahmen, die entweder die Auftretensrate der Gefährdung reduzieren oder die Auswirkungen [der Gefährdung] entschärfen, um ein akzeptierbares Risikolevel zu erreichen und/oder aufrecht zu erhalten*“. (aus dem Englischen nach /62/, Artikel 3). Diese Vorgaben werfen allerdings noch zahlreiche Fragen auf und beinhalten Unklarheiten, so dass hier weiterer Forschungsbedarf besteht.

Für das genannte Beispiel des Bahnübergangs wird davon ausgegangen, dass das zugehörige Risiko zur Gefährdung „BÜ ist nicht gesichert“ nicht allgemein akzeptierbar ist, da in der Regel zusätzliche Sicherheitsmaßnahmen für Strecken mit BÜs vorgeschrieben sind, siehe §11 der EBO (/25/). Im Rahmen dieser Arbeit wird der Aspekt des allgemein akzeptierbaren Risikos jedoch nicht weiter vertieft. Für detailliertere Betrachtungen siehe /88/.

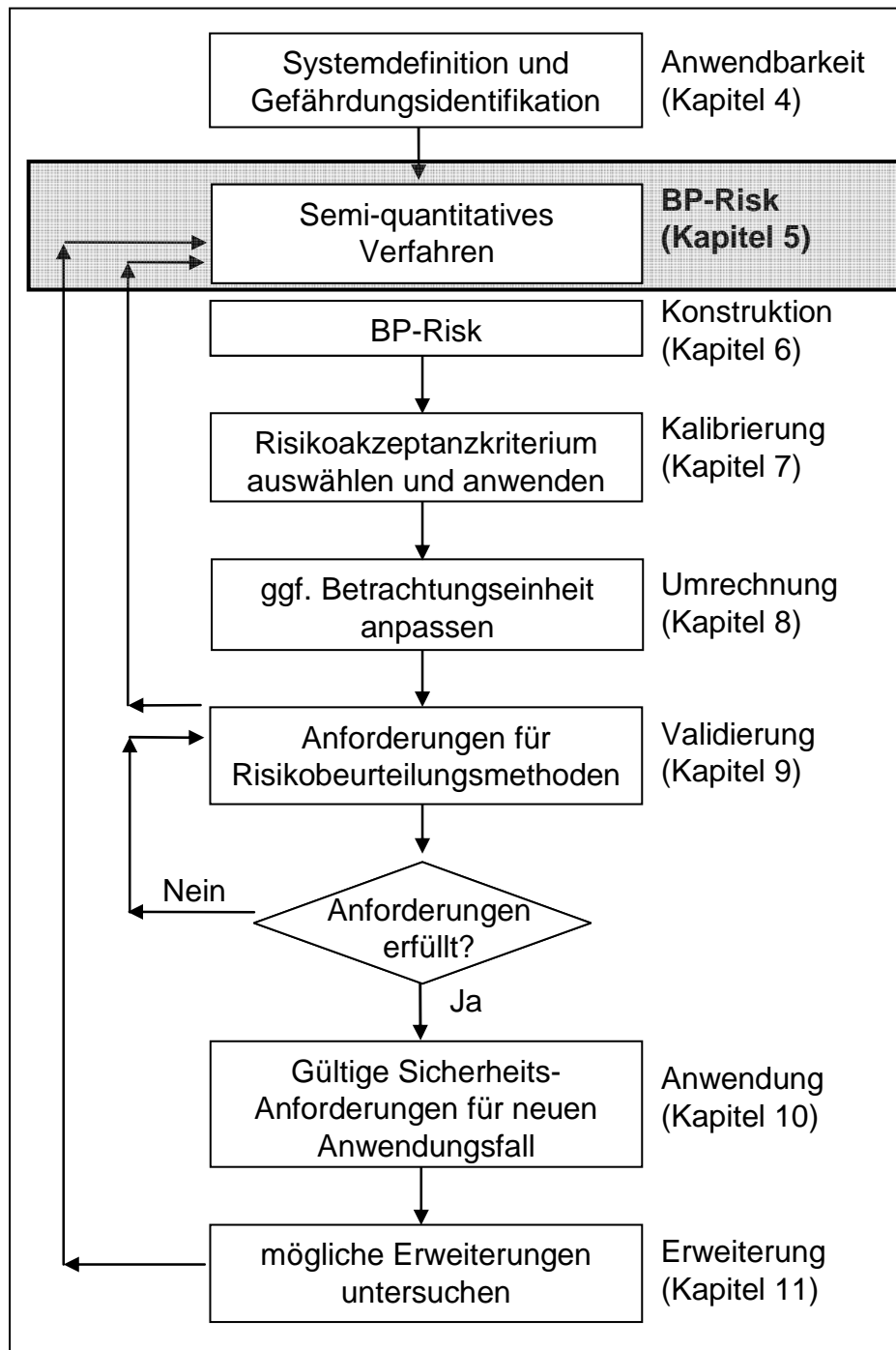
4.4 Zusammenfassung

Ein mit BP-Risk ermitteltes Ergebnis gilt nur in Verbindung mit der Systemdefinition, die unbedingt mit diesem Ergebnis zusammen kommuniziert werden muss. Um diese Kontext-Informationen möglichst einfach weiterzugeben, wurde für BP-Risk eine generische Systemdefinition erstellt, so dass Missbrauch und vor allem falsche Ergebnisse vermieden werden können.

Die generische Systemdefinition wurde auf Grundlage der europäischen Vornorm prEN 00150380-4 für Schienenfahrzeuge erarbeitet und erweitert. Dabei wurde angenommen, dass die prEN 0015380-4 vollständig die Funktionen eines Schienenfahrzeugs beschreibt. Ausgehend von einer vollständigen Schnittstellenbeschreibung für die Leit- und Sicherungstechnik konnten zusätzliche Funktionen auf der von BP-Risk vorgegebenen Ebene ermittelt werden.

Auf Basis der erstellten Funktionsliste für ein Schienenfahrzeug ist eine generische Gefährdungsidentifikation möglich. Dazu können für eine grobe Abschätzung durch Negation der Funktionen die Systemgefährdungen abgeleitet werden. Eine Absicherung kann durch eine zusätzliche systematische Gefährdungsidentifikation erfolgen. Dies wurde in diesem Kapitel anhand einer FMEA beispielhaft für eine BÜ-Sicherungsfunktion gezeigt.

Die erarbeitete Systemdefinition ist nun der Ausgangspunkt für das BP-Risk Risikomodell, was im folgenden Kapitel 5 vorgestellt wird. Darüber hinaus erfolgt eine Erläuterung der Konstruktion von BP-Risk in Kapitel 6.



5 Best Practice Risk (BP-Risk)

Der Begriff ‚best practice‘ stammt aus der angloamerikanischen Betriebswirtschaft und kann nach /90/ mit ‚bestes Verfahren‘ oder ‚bewährte Praxis‘ ins Deutsche übersetzt werden. Es wird oft auch ‚Standardverfahren‘ oder ‚Erfolgsrezept‘ genannt. Wenn ein Unternehmen nach ‚best practice‘ vorgeht, setzt es bewährte und kostengünstige Verfahren ein, die das Unternehmen möglicherweise auf manchen Arbeitsfeldern zum Musterbetrieb für andere machen.

BP-Risk stellt ein optimales Verfahren zur Risikobeurteilung dar, da es anhand von Anforderungen konstruiert wurde, die bisher das ‚best practice‘ zum Thema Risikobeurteilung repräsentieren. BP-Risk eröffnet somit die Möglichkeit, die positiven Eigenschaften von verbreiteten Ansätzen zur Risikobeurteilung zu kombinieren. Dieser neue Ansatz soll eine effiziente und anwenderfreundliche Durchführung der Ableitung von zulässigen Häufigkeiten für Versagen der Funktionen eines Mensch-Maschine-Systems ermöglichen.

5.1 Anforderungen

Tabelle 5-1 Anforderungen im Vergleich

| Nr. | Allgemein | ERA (CSM) | UNIFE (CSM) |
|-----|---|--|---|
| A01 | Risikoakzeptanz: MGS ²⁵ | | Keine höheren Risiken als RAC-TS ²⁶ |
| A02 | Implizites Restrisiko | | |
| A03 | Mensch und Technik Modell | | |
| A04 | Unabhängige Bewertung der Systemfunktionen | | |
| A05 | Qualitative Schadens- und Folgenanalyse | | |
| A06 | Berücksichtigung aller relevanten Parameter | System und Parameter korrekt widerspiegeln | Berücksichtigung aller relevanten Parameter |
| A07 | Genauigkeit innerhalb einer Zehnerpotenz | Genauere Ergebnisse für robuste Entscheidung | Genauigkeit: innerhalb einer Zehnerpotenz |
| A08 | Rigoreuse Begründung der Methode | | Umfassende Dokumentation |
| A09 | | | Ergebnisse: gleiches Format wie Sicherheitsziel |
| A10 | | | Fähigkeit, verschiedene Parameter auszugleichen |
| A11 | | | Überprüfbares Ergebnisdokument |

²⁵ MGS: Mindestens Gleiche Sicherheit (siehe Kapitel 2.1.1).

²⁶ RAC-TS: europäisches Risikoakzeptanzkriterium für Technische Systeme (siehe Kapitel 7.1).

BP-Risk wurde ingenieurmäßig konstruiert. Das bedeutet, dass die Methode aufgrund von Anforderungen entwickelt wurde und zum Schluss nachgewiesen wird, dass diese Anforderungen auch erfüllt worden und in der Praxis plausibel sind. Ein erster Versuch, dieses Prinzip umzusetzen, ist bereits veröffentlicht worden (siehe /9/, Seite 97ff). Dort wurden allgemeine Kriterien aufgestellt, die ein optimales Verfahren zur Risikobeurteilung nach den bisherigen Erkenntnissen erfüllen müsste.

Im Rahmen der Empfehlungen für Common Safety Methods (CSM) hat die ERA ebenfalls Kriterien für Risikobewertungen aufgestellt. Innerhalb der ERA-Arbeitsgruppen zum Thema Common Safety Methods wurden zusätzlich von der Eisenbahnindustrie (UNIFE) detaillierte Anforderungen für effiziente Verfahren zur Risikobeurteilung vorgeschlagen. Tabelle 5-1 zeigt die gesammelten Anforderungen im Vergleich.

Da die CSM-Anforderungen zum Teil den allgemeinen Anforderungen entsprechen, sie aber auch ergänzen, werden die gültigen Anforderungen für BP-Risk in Tabelle 5-2 zusammengefasst und eine Obermenge gebildet. Diese bildet die Grundlage der Validierung im Rahmen dieser Arbeit. Dabei wird angenommen, dass die genannten Anforderungen anerkannt und nicht widersprüchlich sind. Ausformulierungen der einzelnen Anforderungen und weitere Erläuterungen finden sich in Kapitel 9.

Tabelle 5-2 Anforderungen für BP-Risk

| Nr. | Anforderungen |
|-----|--|
| A01 | Risikoakzeptanz: keine höheren Risiken als RAC-TS |
| A02 | Implizites Restrisiko |
| A03 | Mensch und Technik Modell |
| A04 | Unabhängige Bewertung der Systemfunktionen |
| A05 | Qualitative Schadens- und Folgeanalyse |
| A06 | Berücksichtigung aller relevanten Parameter |
| A07 | Genauigkeit innerhalb einer Zehnerpotenz |
| A08 | Rigorese Begründung der Methode; umfassende und überprüfbare Dokumentation |
| A09 | gleiche Einheiten und Betrachtungsgegenstand von Sicherheitsziel und Ergebnissen |
| A10 | Fähigkeit, verschiedene Parameter auszugleichen |

Der Nachweis, dass diese Anforderungen erfüllt sind, erfolgt im Rahmen der Validierung in Kapitel 9 dieser Arbeit. Im Folgenden werden nun das Grundmodell und die Konstruktionsprinzipien von BP-Risk auf Basis der genannten Anforderungen und der im vorigen Kapitel 4 erarbeiteten Systemdefinition vorgestellt.

5.2 Konstruktionsprinzip

Die Konstruktion von BP-Risk vollzieht sich in drei Schritten (siehe Abbildung 5-1). Da ein erster vorläufiger Ansatz von BP-Risk bereits veröffentlicht wurde, werden im Folgenden die Grundsätze nur noch einmal kurz wiedergegeben und erläutert. Die vorliegende Arbeit legt dabei den Fokus auf die Änderungen, die sich rückwirkend aus den genannten europäischen Anforderungen, der neuen Kalibrierung (siehe Kapitel 7), der Validierung (siehe Kapitel 9) und aus der Anwendung der Methode ergeben haben.

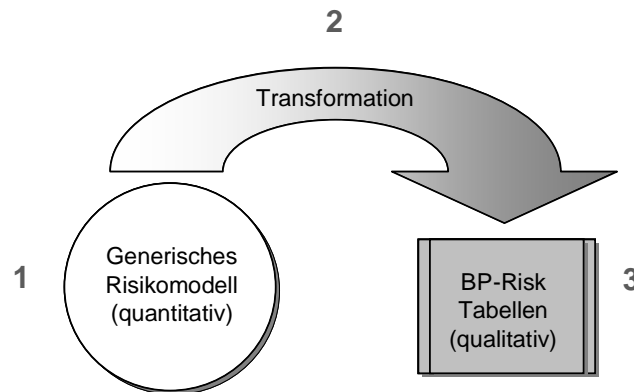


Abbildung 5-1 BP-Risk Konstruktion

1) Generisches Risikomodell

Beim grundlegenden BP-Risk Ansatz wird zunächst ein probabilistisches Modell definiert, das die relevanten Parameter und Annahmen enthält (generisches Risikomodell). Dieses Modell ist gut geeignet für Systeme mit geringer Komplexität bzw. für hohe Systemlevel von allgemeinen Systemen. Für diese Systeme können das Schadensausmaß und die Eintrittswahrscheinlichkeit sowie die Wahrscheinlichkeit der Fehleroffenbarung für ein bestimmtes Funktionsversagen direkt analysiert werden (siehe Kapitel 5.3).

2) Transformation

Das probabilistische Modell wird dann mittels einer mathematischen Transformation, die die wesentlichen Eigenschaften des Modells (Monotonie, Vergleichbarkeit, Einfachheit) enthält, auf ein qualitatives Modell abgebildet. Dabei werden die quantitativen Parameter diskretisiert (gerundet) und auf Parameterbereiche abgebildet (siehe Kapitel 5.4).

3) BP-Risk Tabellen

Die Parameterbereiche müssen hinsichtlich der Minimierung von Diskretisierungsfehlern und der sinnvollen verbalen Beschreibung optimiert werden. Bei der qualitativen Beschreibung der BP-Risk-Tabellen fanden im Rahmen dieser Arbeit die meisten Anpassungen statt. Deswegen werden diese in einem gesonderten Kapitel behandelt (siehe Kapitel 6).

5.3 Generisches Risikomodell

Das generische Risikomodell betrachtet ein Eisenbahnsystem (ein Zug), das Mensch und Technik umfasst und aus verschiedenen Teilfunktionen besteht. Diese Teilfunktionen können versagen, so dass das System mehrere Funktionsversagen (Ausfallmodi) $i = 1, \dots, n$ besitzt. Jedes Funktionsversagen ist verbunden mit einem gewissen Risiko. Für das probabilistische Risikomodell wird davon ausgegangen, dass die Teilrisiken, die durch die Funktionsversagen des Systems entstehen, additiv sind, d. h. das zum System zugehörige Gesamtrisiko R ist nicht größer als die Summe der Teilrisiken R_i :

$$R \leq \sum_{i=1}^n R_i \quad \text{Gleichung 5-1}$$

Die Addition von Risiken ist allerdings nicht präzise, weil als Voraussetzung für eine Addition die Risiken disjunkt²⁷ sein müssen. In der Praxis sind sie es jedoch nicht. Diese Annahme lässt sich allerdings in der Regel auf einer genügend hohen Systemebene rechtfertigen, so dass die Gefährdungen sich vernachlässigbar überlappen und das Gesamtrisiko zur sicheren Seite abgeschätzt werden kann. Der Anwendungsbereich des BP-Risk-Ansatzes beschränkt sich daher auf ein relativ hohes Systemniveau.

Ferner wird angenommen, dass die verschiedenen Teilfunktionen mit einer Häufigkeit f_i versagen und somit zu einer Gefährdung führen können. Dabei wird vereinfachend davon ausgegangen, dass auf einer relativ hohen Systemebene ein Funktionsversagen einer Systemgefährdung entspricht. Die Wahrscheinlichkeit für das Auftreten einer Systemgefährdung wird außerdem in Abhängigkeit von der möglichen Gefahrenabwehr g_i formuliert. So beschreibt g_i die mittlere Wahrscheinlichkeit, dass die Fehleroffenbarung oder die Gefahrenabwehr (Möglichkeit den Unfall zu verhindern) versagt. CENELEC definiert Risiko als „*Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens*“ (/30/). Das Schadensausmaß s_i beschreibt demnach den Schweregrad eines aus der Systemgefährdung resultierenden Unfalls (nachdem die Gefahrenabwehr versagt hat).

Der Ansatz der Teilrisiken wird in Anlehnung an den RPN-Ansatz formuliert, nämlich dass die oben genannten Parameter das Teilrisiko R_i multiplikativ beeinflussen. Die Multiplikation setzt voraus, dass die Parameter unabhängig voneinander sind.

$$R_i = f_i \cdot g_i \cdot s_i \quad \text{Gleichung 5-2}$$

Zusätzlich wird beim Ansatz des Teilrisikos nur ein Unfallszenario berücksichtigt. Es wird hier der schwerste, jedoch noch glaubwürdigste Schadensfall mit dem größten Risikowert angenommen. Für BP-Risk wird somit ein realistisches Unfallszenario berücksichtigt, statt die Summe der Produkte aus Unfallwahrscheinlichkeit und Unfallschwere, wie es beispielsweise

²⁷ disjunkt: kein gemeinsames Element aufweisend (elementfremd); untereinander verschieden (/89/).

bei einem Ereignisbaum²⁸ üblich ist. Wichtig dabei ist, dass nicht der ‚worst-case‘-Pfad angenommen wird, wie es z. B. in der DIN 62061 (Maschinensicherheit) gefordert wird. *„Nach den Erfahrungen in der Eisenbahntechnik tendieren selbst erfahrene Experten dazu, bei Worst-Case-Betrachtungen die betrieblichen Folgen grundsätzlich zu negativ zu bewerten, so dass die (wirtschaftliche) Gefahr einer zu teuren Entwicklung besteht“* (/68/). Um die Balance zwischen der notwendigen Sicherheit und dem wirtschaftlichen Aufwand zu halten, wird deshalb bei BP-Risk der Ansatz der typischen Folgenabschätzung gewählt.

Mit Hilfe von BP-Risk soll die zulässige Versagenshäufigkeit der jeweiligen Systemgefährdung bzw. des jeweiligen Funktionsversagens ermittelt werden. Der Grundansatz besteht darin, für jede einzelne Systemgefährdung eine vereinfachte Folgen- und Schadensbewertung durchzuführen. Für die jeweilige Systemgefährdung erfolgt somit eine Abschätzung der möglichen Gefahrenabwehr und des typischen Schadensausmaßes. Die charakteristischen Umwelteinflüsse, Rahmenbedingungen und Vermeidungsmöglichkeiten (Barrieren), die ‚zwischen‘ dem Funktionsversagen und einem möglichen Schadensereignis stehen, werden bewertet (siehe Abbildung 5-2). Mit Hilfe eines Risikoakzeptanzkriteriums kann dann die tolerierbare Versagenshäufigkeit für die betrachtete Systemgefährdung ermittelt werden.

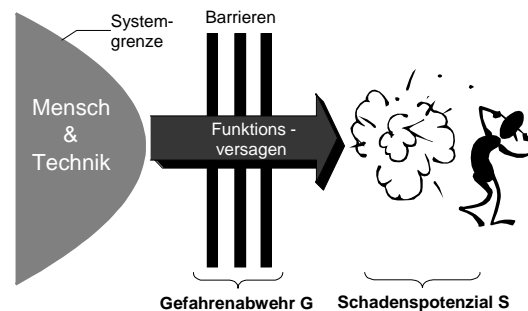


Abbildung 5-2: Funktionsversagen des Mensch-Maschine-Systems (nach /9/, S. 100)

Die Parameter des Teilrisikos können sich ihrerseits wieder aus weiteren Parametern zusammensetzen; so wird im Folgenden die Gefahrenabwehr g und das Schadensausmaß s mit Hilfe von Subparametern beschrieben. Diese Subparameter stellen dabei die relevanten Einflüsse dar, die im Bereich der Konsequenzanalyse die Bewertung des Risikos bestimmen. Dieser Ansatz hat den Vorteil, dass nicht mehr direkt die Gefahrenabwehr oder das Schadensausmaß geschätzt werden müssen, sondern Subparameter benutzt werden, die vom Anwender einfacher beurteilt werden können.

Der multiplikative Ansatz des Teilrisikos wird auch für die Subparameter übernommen und setzt somit voraus, dass diese ebenfalls unabhängig voneinander sind. Dieser Aspekt spielt vor allem bei der Beschreibung der BP-Risk Tabellen (siehe Kapitel 6) eine Rolle, da die Subparameter der Parameter g und s unabhängig voneinander beschrieben und bewertet werden müssen.

²⁸ Ereignisbaumanalyse (ETA): eine bei der Risikoanalyse häufig eingesetzte Methode zur Beurteilung der Folgen von Ereignissen, die durch ein erstes Ereignis ausgelöst werden (siehe DIN 25419).

5.3.1 Gefahrenabwehr g

Mit Hilfe des Parameters Gefahrenabwehr wird eine vereinfachte Folgenanalyse durchgeführt. Somit werden die möglichen Konsequenzen bewertet, die sich aus einer Gefährdung ergeben können. Da nicht alle Gefährdungen unmittelbar zu Unfällen führen, werden vor allem die verschiedenen Schutzmaßnahmen identifiziert und beurteilt. Die Subparameter für die Gefahrenabwehr berücksichtigen deshalb Maßnahmen zur Verhinderung von Unfällen und zur Reduzierung des resultierenden Schadens. Diese Ereignisse oder Gegebenheiten müssen jedoch explizit außerhalb des definierten Systems liegen.

Nach /9/ (Seite 103) zählen zur Gefahrenabwehr:

- die betrieblichen Randbedingungen b_i ,
- die menschlichen Handlungen m_i , die nicht dem System zugerechnet werden können oder nicht planmäßig erfolgen (Regelhandlungen) sowie
- die Dauer der Gefährdung d_i .

Der Parameter d wird auch in der Risikoformel verwendet, wo er jedoch einem anderen Risikomodell unterliegt und somit eine andere Bedeutung hat als bei BP-Risk. Dies wird im folgenden Exkurs näher erläutert.

Exkurs: Gefährdungsdauer

Im Rahmen der Risikoformel wird ein Individuum betrachtet, das einer Gefährdung eines technischen Systems (z. B. eines ungesicherten Bahnübergangs) ausgesetzt ist. Das Individuum (z. B. ein Straßenverkehrsteilnehmer) kann der Gefährdung begegnen, sobald das Funktionsversagen eingetreten ist und die Gefährdungsdauer beginnt. So lange die Gefährdung andauert, ist es für das Individuum möglich, dieser Gefährdung zu begegnen. Dies ist dann nur noch abhängig von der Aussetzungsdauer - wie oft und wie lange sich das Individuum im Gefahrenbereich aufhält (beispielsweise wie oft und wie lange der Straßenverkehrsteilnehmer den nicht gesicherten Bahnübergang überquert).

Die Gefährdungsdauer ist somit nur relevant, um die Möglichkeit zu bewerten, dass die Gefährdung erst gar nicht auftritt, sondern das Funktionsversagen (beispielsweise durch Wartung oder Tests) offenbart werden kann, bevor die Funktion erbracht oder genutzt wird. Die Gefährdungsdauer ist allerdings nicht mehr relevant, wenn es um die Risikoreduktion des Unfalls geht, da in diesem Fall die Gefährdung schon vorliegt und nur noch bewertet wird, inwiefern der Schaden zu verhindern oder zu verringern ist. Diese Vorgehensweise ist bei BP-Risk der Fall.

Wie oben erwähnt, kann die betriebliche Dauer der Gefährdung auch dem Prüfzyklus entsprechen, mit dem ein Funktionsversagen z. B. durch Wartungsarbeiten oder Funktionstests offenbart und damit beseitigt wird. Die Wartungsintervalle werden im Rahmen von BP-Risk allerdings nicht berücksichtigt, da nur eine Zugstunde (Zugfahrt von einer Stunde Dauer)

betrachtet wird und davon auszugehen ist, dass die Wartungsintervalle deutlich über einer Stunde liegen. So ist die Wahrscheinlichkeit, dass die Wartung in die betrachtete Stunde fällt, vernachlässigbar klein. Das bedeutet, dass ein Funktionsversagen in der Regel durch Nutzung und nicht durch Wartung offenbart wird.

Der Parameter d würde im Rahmen von BP-Risk nur zur Gefahrenabwehr beitragen, wenn das Funktionsversagen offenbart wird, bevor der betrachtete Zug die Funktion nutzt (fahrzeugseitig) oder dem Funktionsversagen (streckenseitig) begegnet. Fahrzeugseitig wirkt sich ein Funktionsversagen also sofort als Gefährdung aus, da das Versagen nur durch Nutzung erkannt werden kann. Ein Bremsversagen wird beispielsweise nur offenbart, wenn der Zug die Bremsfunktion nutzt. Somit spielt hier die Gefährdungsdauer keine Rolle. Streckenseitig ist die Gefährdungsdauer nur relevant, wenn die Gefährdung durch einen anderen Zug offenbart werden kann. Hierbei spielt die Belastung (wie viele Züge pro Stunde sich auf dem betrachteten Streckenabschnitt befinden) eine Rolle.

Um einen Anhaltspunkt für die streckenseitige Gefährdungsdauer zu bekommen, wurde die mittlere, maximale Belastung (Zug/h) für die jeweilige Streckenkategorie aus den DB-Streckenstandards (siehe auch Anhang D: Streckenstandards) herangezogen. Es kann somit die Zeit errechnet werden, die durchschnittlich zwischen zwei Zügen vergeht. Diese wird als mittlere Gefährdungsdauer d im Sinne von BP-Risk angenommen. Die Werte aus Tabelle 5-3 zeigen, dass im Personenverkehr die mittlere Gefährdungsdauer unterhalb einer Stunde liegt. Hier werden jedoch die Tagesganglinien vernachlässigt, da ein Mittelwert der Belastung berechnet wurde. Insgesamt kann jedoch festgestellt werden, dass die Werte bis auf Ausnahmen in Relation zur Betrachtungseinheit klein sind. Insofern wird zur sicheren Seite die streckenseitige Gefährdungsdauer gleich der Betrachtungszeit (eine Stunde Zugfahrt) gesetzt und nicht weiter als Subparameter der Gefahrenabwehr differenziert.

Tabelle 5-3 Gefährdungsdauer d

| Strecken-Standard | maximale Belastung | Gefährdungsdauer d | |
|-------------------|--------------------|----------------------|-----------|
| | | [h/Zug] | [min/Zug] |
| HGV | 5,00 | 0,20 | 12,00 |
| SPFV230 | 3,86 | 0,26 | 15,54 |
| SPFV160 | 3,05 | 0,33 | 19,65 |
| SPNV120 | 2,06 | 0,48 | 29,09 |
| SPNV80 | 1,33 | 0,75 | 45,00 |
| SGV | 0,42 | 2,40 | 144,00 |

In Anlehnung an Gleichung 5-2 wird die Möglichkeit zur Gefahrenabwehr somit als Funktion der Subparameter b und m dargestellt:

$$g_i = b_i \cdot m_i \quad \text{Gleichung 5-3}$$

5.3.2 Schadensausmaß s

Im zivilrechtlichen und volkswirtschaftlichen Bereich gehen die Bemühungen dahin, für alle Schäden eine monetäre Bewertung zu entwickeln. Aus ethischer Sicht bestehen jedoch Bedenken, Unfalltod oder Körperschäden bzw. den Verlust ideeller Werte in Geldwert aufzurechnen. Das Verlangen, alle Schäden finanziell zu bewerten, führt zu Motivationskonflikten, die sich so beschreiben lassen: *„Wird das wirtschaftliche Optimum für alle Schäden angestrebt, muss oft ein bestimmtes Ausmaß an Sach- und Personenschäden in Kauf genommen werden. Vom Standpunkt der Humanität aus ist jedoch anzustreben, gerade Personenschäden möglichst gering zu halten. Das führt dazu, dass der durch eine technische Anlage oder durch eine Technologie bedingte ‚Schaden‘, gemessen durch sein finanzielles Äquivalent, nicht mehr minimal sein kann. Der Konflikt liegt darin, zu entscheiden, wieweit das wirtschaftliche Minimum verlassen werden soll zugunsten einer verringerten Anzahl zu erwartender Personenschäden. Diese Aufgabe ist von der Sicherheitswissenschaft allein nicht zu lösen [...]“* (/85/, Seite 8).

Für das generische Risikomodell von BP-Risk wird das Schadensausmaß nicht monetär, sondern anhand von Personenschäden bewertet. Als Personenschaden wird ein Ereignis mit Todesfolge bzw. Verletzung einer Person oder mehrerer Personen bezeichnet. Die Schadensbewertung erfolgt nach der Folgenanalyse, d. h. sie betrachtet den Fall, dass die Barrieren der Gefahrenabwehr durchbrochen wurden und es zu einem Schadensereignis kommt.

Für BP-Risk bildet die Formel der kinetischen Energie (Gleichung 5-4) die Grundlage der Schadensbewertung. Nach /65/ hängt das Risiko bei Transportprozessen ab von der kinetischen Energie E der bewegten Masse m mit der Geschwindigkeit v , für die gilt:

$$E = \frac{1}{2} \cdot m \cdot v^2 \quad \text{Gleichung 5-4}$$

Auch in /109/ wird die Grundlage der kinetischen Energie genannt und zusätzlich ausgesagt, dass die Höhe des Unfallschadens wesentlich von der Fahrzeuggeschwindigkeit abhängig ist. Da Personenschäden als Bezugsgröße definiert wurden, wird angenommen, dass der Schaden eines Unfalls neben der kinetischen Energie E abhängig ist von der Anzahl der betroffenen Personen a_i (für das betrachtete Funktionsversagen i). Somit kann der Schweregrad s_i ausgedrückt werden durch:

$$s_i = E_i \cdot a_i \quad \text{Gleichung 5-5}$$

Gleichung 5-4 in Gleichung 5-5 eingesetzt und für BP-Risk angepasst ergibt:

$$s_i = \frac{1}{2} \cdot t_i \cdot v_i^2 \cdot a_i \quad \text{Gleichung 5-6}$$

In dieser Gleichung 5-6 steht t_i für die mittlere Masse in Abhängigkeit der Zuggattung, v_i^2 für die mittlere quadratische Geschwindigkeit des Zuges und a_i für die Anzahl der betroffenen

Personen in Abhängigkeit des Unfalltyps. Der konstante Wert $\frac{1}{2}$ entfällt durch die Kalibrierung der BP-Risk Tabellen und wird im Folgenden nicht weiter berücksichtigt.

Als Einheit für das Schadensausmaß ergibt sich die kinetische Energie, die auf die betroffenen Personen wirkt. Da die kinetische Energie nach /65/ vor allem in Verformungsenergie umgewandelt wird, kann die Einheit ‚Energie * Personen‘ interpretiert werden als geschädigte (verletzte) Personen oder auch Opfer.

5.4 Transformation

Die Risikobewertung anhand eines probabilistischen Risikomodells (wie z. B. bei der Risikoformel) beinhaltet meist komplexe Rechnungen durch Ausweisung des expliziten Risikos und ebenso durch die Auswahl von absoluten Bewertungskriterien. Für BP-Risk erfolgt statt der Ausweisung des expliziten Risikos eine Kritikalitätsbewertung der jeweiligen Funktionsversagen. Die Kritikalität K ist nach /19/ eine subjektive Maßeinheit für das Risiko und wird definiert als eine Kombination aus Schaden und Eintrittshäufigkeit eines Ereignisses.

Um die Kritikalität K zu beschreiben, wird eine mathematische Transformation mit definierten Eigenschaften für das oben vorgestellte Risikomodell durchgeführt. Dabei ist K_i nichts anderes als eine verbesserte RPN, die die Kritikalität eines Ausfalls beschreibt. Durch die Transformation wird eine neue Definition der RPN aufgestellt, die als eine Funktion der Parameter f , g , und s die folgenden Eigenschaften erfüllt:

- Monotonie: für zwei Funktionsversagen m und n gilt $K_m \leq K_n$, wenn $R_m < R_n$.
- Vergleichbarkeit: für zwei Funktionsversagen m und n gilt $K_m = K_n$, wenn $R_m \approx R_n$.
- Einfachheit: die Rechnungen sollten einfach durchzuführen sein.

Basierend auf diesen Anforderungen scheint sich eine logarithmische Funktion anzubieten, da diese eine monotone Transformation und einfache Rechenergebnisse liefert. In der Literatur (/113/, /70/) findet man bei qualitativen oder semi-quantitativen Methoden ebenfalls die Anwendung von logarithmierten Skalen, um sicherzustellen, dass die Parameterwerte gleiche Abstände haben. Der Ansatz für verbesserte Risikoprioritätszahlen (RPN) verwendet ebenfalls eine logarithmische Transformation. /7/ hat gezeigt, dass diese logarithmische Transformation vorteilhafte Eigenschaften hat und über eine einfache Operation (nämlich Addition statt Multiplikation) zu einer elementaren Rechnung führt.

Für BP-Risk wird das oben vorgestellte Risikomodell transformiert, indem Gleichung 5-2 logarithmiert wird und man somit die zu jedem Teilrisiko zugeordnete Kritikalität K_i erhält:

$$K_i = [\log_x(R_i)] = [\log_x(f_i)] + [\log_x(g_i)] + [\log_x(s_i)] \quad \text{Gleichung 5-7}$$

Die weiterführenden Ausdrücke für die Gefahrenabwehr und das Schadensausmaß lassen sich somit ebenfalls mathematisch transformieren. Für die Parameter g aus Gleichung 5-3 und Parameter s aus Gleichung 5-6 ergeben sich:

$$\log_x(g_i) = \log_x(b_i) + \log_x(m_i)$$

Gleichung 5-8

$$\log_x(s_i) = \log_x(t_i) + 2 \times \log_x(v_i) + \log_x(a_i)$$

Gleichung 5-9

Zusätzlich werden die Ausdrücke gerundet, um natürliche Zahlen in den BP-Risk Tabellen zu erhalten. Als Ergebnis der Transformation folgt, dass jeder Grundparameter auf einer ganzzahligen Skala abgebildet wird. Die Skalen können so transformiert werden, dass immer ein Bereich zwischen 1, ... y gewählt werden kann. Die Breite y der Skala ist in der Regel für jeden Parameter unterschiedlich (siehe auch Kapitel 6).

Der absolute Unterschied zwischen benachbarten Werten muss in allen Skalen jedoch immer der gewählten logarithmischen Basis x entsprechen. Die empfohlene Basis x beträgt $\sqrt[3]{10} \approx 3,2$. In anderen Risikobetrachtungen (z. B. /70/) wird oft die Basis 10 zugrunde gelegt, damit die Tabellenwerte mit einem Wert von 10 auseinander liegen. Die Basis $\sqrt[3]{10}$ wurde deswegen gewählt, um feinere Abstufungen zu erreichen. Außerdem wird im Vergleich zur Basis 10 der Einschätzungsfehler bei Basis $\sqrt[3]{10}$ kleiner, da sich beim nächst größeren bzw. nächst kleineren Tabellenwert betragsmäßig ein Fehler von $\sqrt[3]{10} \approx 3,2$ statt 10 ergibt.

Die Skalenverschiebung ist so gewählt, dass die Rundungsfehler möglichst klein und gleichmäßig verteilt sind. Eine europäische Anforderung für effiziente Risikoanalysen lautet, dass die Aussagegenauigkeit (Rundungs- und Einschätzungsfehler) des Verfahrens innerhalb einer Zehnerpotenz liegen sollte. Dafür ist die Basis $x = \sqrt[3]{10}$ ebenfalls gut geeignet, da diese Genauigkeitsanforderung dann einer Differenz von ± 1 in der Kritikalität K entspricht. Detailliertere Erklärungen zur Genauigkeitsanforderung finden sich in Kapitel 9.8.

Die Formel für die Kritikalität, für die Gefahrenabwehr sowie für das Schadensausmaß können nun einfacher geschrieben werden:

$$K_i = F_i + G_i + S_i$$

Gleichung 5-10

$$G_i = B_i + M_i$$

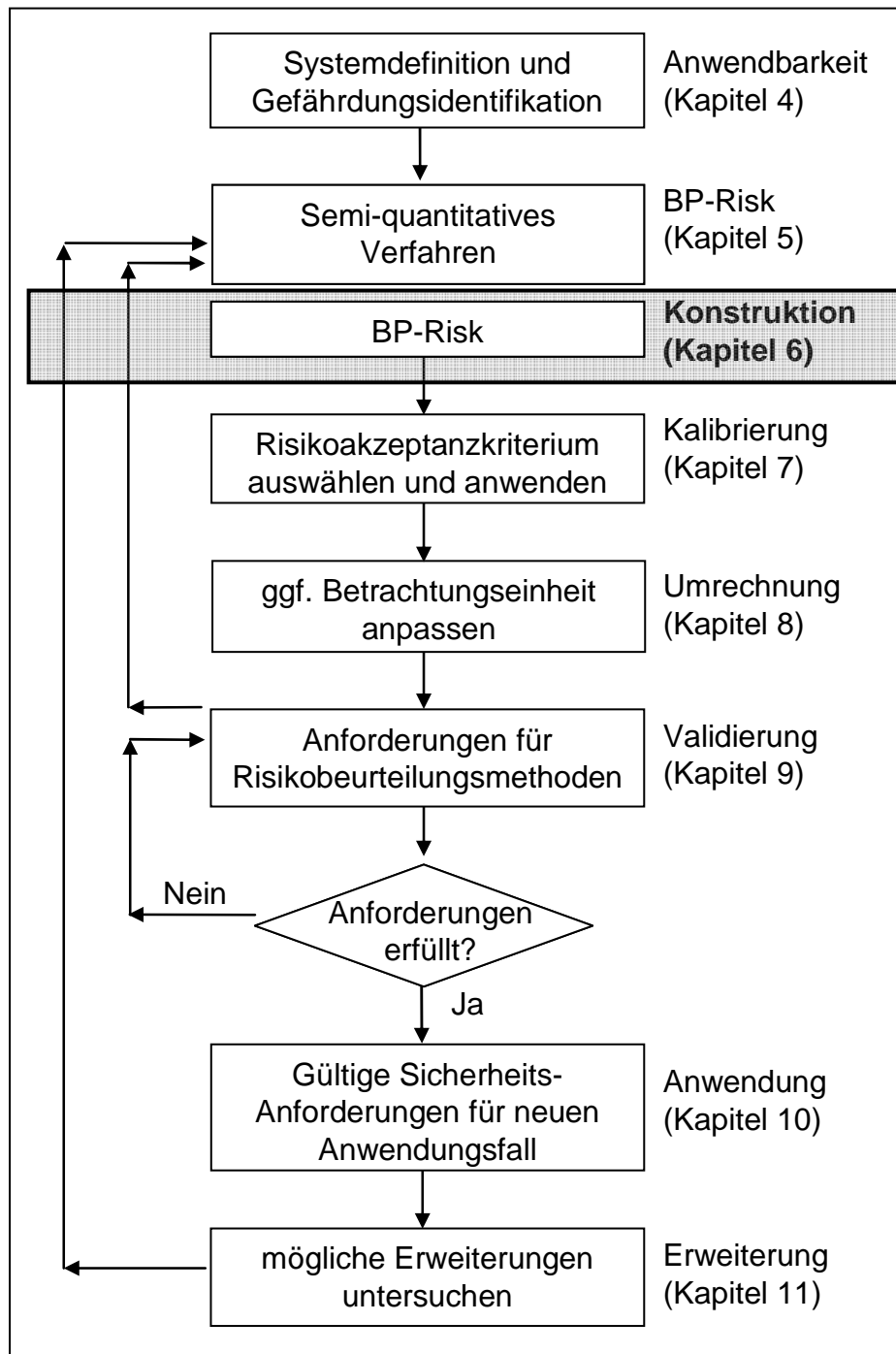
Gleichung 5-11

$$S_i = T_i + V_i + A_i$$

Gleichung 5-12²⁹

Um dem Anwender ein möglichst einfaches Verfahren an die Hand zu geben, werden die transformierten Parameter des Risikomodells auf vordefinierte Parameterbereiche abgebildet. Dies erfolgt anhand von Tabellen, die in einem ersten Ansatz von BP-Risk bereits veröffentlicht wurden (siehe /9/, Seite 97ff). Im Rahmen der Validierung ergaben sich jedoch rückwirkend Anforderungen an die Konstruktion und die Anwendbarkeit von BP-Risk, so dass das Verfahren entsprechend angepasst wurde. Die Konstruktion der BP-Risk Tabellen ist im folgenden Kapitel 6 ausführlich beschrieben, da sie die Basis der Anwendung und der Validierung liefern.

²⁹ Der Ausdruck $2 \times \log(v_i)$ wird zusammengefasst zu V_i und der Wert 2 fließt in der Kalibrierung der BP-Risk Tabellen mit ein.



6 Konstruktion

Auf der Grundlage des im Kapitel 5.3 beschriebenen Modells soll im Rahmen von BP-Risk eine vereinfachte Risikobewertung erfolgen, welche die Bestimmung der Parameter Gefahrenabwehr (G) und Schadensausmaß (S) einbezieht. Nach einer detaillierten Betrachtung zu jedem der Parameter greift der Anwender auf der jeweiligen Skala den passenden Parameterwert ab. Nach der Addition der Parameter G und S kann die zulässige Versagenhäufigkeit der zugehörigen Funktion aus einer Tabelle abgelesen werden. Der grundsätzliche Ablauf des BP-Risk Verfahrens ist in Anlehnung an die Empfehlungen für CSMs in Abbildung 6-1 dargestellt.

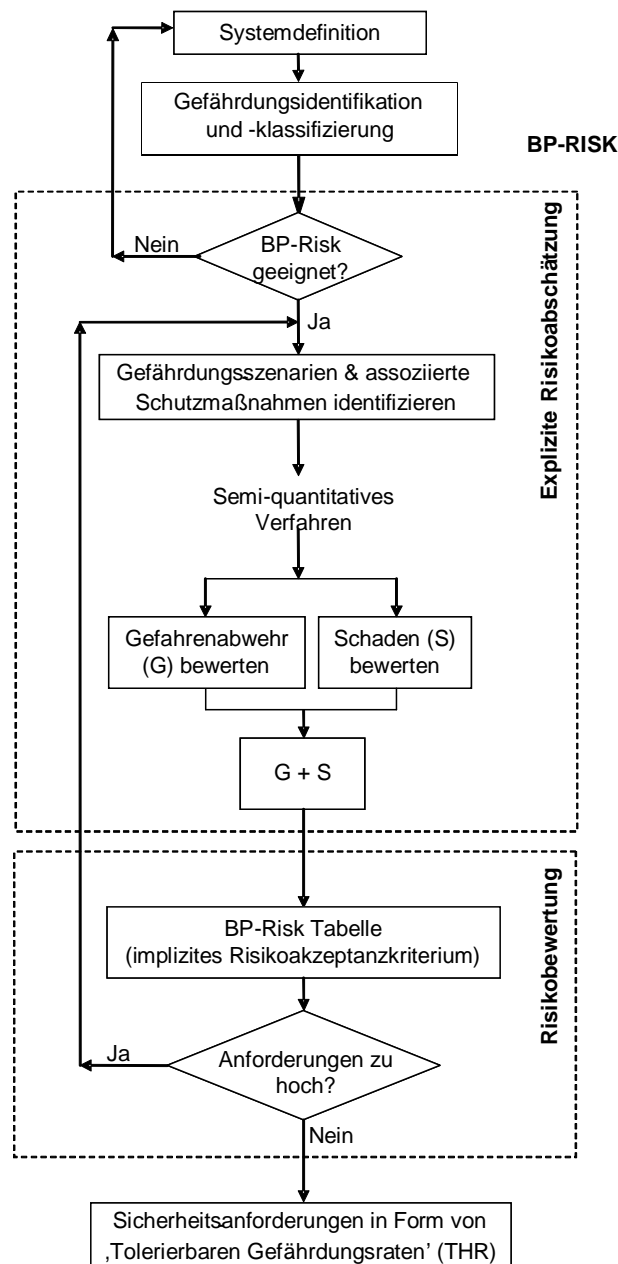


Abbildung 6-1 Ablauf der BP-Risk-Analyse

Grundsätzlich erfolgt die Konstruktion der BP-Risk Tabellen nach bestimmten Kriterien. Zunächst sollen die Ausdrücke gerundet werden, um natürliche Zahlen in den BP-Risk Tabellen zu erhalten. Der absolute Unterschied zwischen benachbarten Werten soll in allen Skalen immer der gewählten logarithmischen Basis $\sqrt[10]{10}$ entsprechen.

Durch die Auswahl der Skalennullpunkte und der qualitativen Beschreibung der Parameterbereiche erhält man ein Bewertungsverfahren mit einfacher Rechnung, das statt absoluten Bewertungskriterien relative Parameterwerte benutzt und das Risiko implizit enthält. Die Nullpunkte der Skalen sind so zu legen, dass die Rundungsfehler möglichst gleichmäßig verteilt sind. Die Skalenanfänge sollen bei Eins liegen, da der Wert Null häufig als ‚Nichts‘ oder ‚hat keinen Einfluss‘ interpretiert wird. Da die Skalen hinsichtlich ihres Nullpunktes beliebig verschoben werden können, ist erkennbar, dass Konstanten in diesem Ansatz keine Rolle spielen.

Für jede Systemgefährdung erfolgt eine Abschätzung des typischen Schadensausmaßes sowie der möglichen Gefahrenabwehr. Es ist hierbei von entscheidender Bedeutung, dass für die Bewertung keine ‚worst-case‘-Situationen angenommen werden, sondern durchschnittliche oder typischerweise auftretende Gegebenheiten. Ein Abweichen würde eine falsche Einstufung der zulässigen Versagenshäufigkeit zur Folge haben und das Verfahren würde zu überzogenen Forderungen führen. Erfahrungen aus vorangegangenen Analysen zeigen, dass Anwender dazu neigen, zur sicheren Seite abzuschätzen, wenn sie keine oder wenige Informationen über die einzuschätzenden Subparameter haben. Um diese worst-case‘-Szenarios zu vermeiden, müssen die Tabellen möglichst genau beschrieben und wenn möglich mit Beispielen versehen werden.

Folglich sollen den Skalenwerten relativ pragmatische und eindeutige Beschreibungen für die einzelnen Skalenwerte zugeordnet werden. Subjektive Beschreibungen werden erleichtert, wenn qualitative Bewertungsmaßstäbe zugelassen werden. Beispielsweise ist es einfacher, anhand zahlreicher Modellexperimente und Analogieüberlegungen, eine heftige Explosion als ‚äußert unwahrscheinlich‘ zu bezeichnen, als ihr z. B. die Wahrscheinlichkeit 0,0001 zuzuordnen. In der Regel täuschen quantitative Werte auch eine Genauigkeit vor (hier z. B. vier Nachkommastellen), die die Methode gar nicht erfüllen kann. Deswegen werden für BP-Risk die Parameterwerte qualitativ beschrieben und mit Beispielen aus der Eisenbahnpraxis erläutert.

Dabei ist zu beachten, dass die Beispiele unabhängig von den anderen Risikoparametern genannt werden. In den bereits veröffentlichten Tabellen (/9/, Seite 97ff) wurde z. B. die Anzahl betroffener Personen mit dem Beispiel eines Unfalltyps beschrieben, was vermieden werden sollte, da es eine Abhängigkeit erzeugt und den Anwender einschränken könnte. Bei der Beschreibung der Tabellen muss also darauf geachtet werden, dass die Parameter nicht abhängig voneinander formuliert werden, so dass der Anwender jeden Parameter für sich betrachtet.

Zusammenfassend liefern die genannten Kriterien folgende Anforderungen für die Beschreibung der BP-Risk Tabellen:

- Werte runden, um natürliche Zahlen zu erhalten,
- Faktor zwischen zwei benachbarten Werten entspricht $\sqrt[3]{10}$,
- Skalennullpunkte auswählen (kleiner Rundungsfehler und Beginn bei ‚Eins‘),
- genaue, qualitative Beschreibungen den Skalenwerten zuordnen (mit unabhängigen Beispielen).

Im Folgenden wird näher auf die einzelnen Parameter eingegangen, wobei die jeweiligen Skalen erläutert werden. Die Tabellen sind grundsätzlich nach folgendem Prinzip aufgebaut (siehe Tabelle 6-1):

Tabelle 6-1 Aufbauprinzip der BP-Risk Tabellen

| Abkürzung | x | log x | Rf | X | Trans. | Qual. Beschr. | Bsp. |
|--------------|--------------------|---------------------------------|---|--------------------------------|---|--------------------------|-----------|
| für Anwender | nicht sichtbar | | | | sichtbar | | |
| Erläuterung | Quantitativer Wert | Logarithmus zur Basis Wurzel 10 | Absoluter Rundungsfehler $Rf = X - \log x$ | Ganzzahliger (gerundeter) Wert | Transformierter Wert (Verschiebung des Skalennullpunkts) | Qualitative Beschreibung | Beispiele |

Das Ziel von BP-Risk in Bezug auf die Anwendbarkeit ist, dass der Anwender nur die einfachen Tabellen korrekt anwenden muss, weil er darauf vertraut, dass die Konstruktion des Verfahrens richtig ist. Die eigentliche Anwendung von BP-Risk ist nicht schwierig, da das Verfahren mit Absicht so konstruiert wurde, dass es möglichst einfach zu handhaben ist. Allerdings muss dabei beachtet werden, dass eine Methode niemals das (Mit-)Denken des Anwenders ersetzen kann. Falls also beispielsweise betriebliche Bedingungen unklar sind und der Anwender möglicherweise keine passende Parametereinstufung finden kann, müssen Annahmen getroffen und dann als Anforderung definiert werden.

6.1 Gefahrenabwehr

Hinzen beschreibt zwischen Gefährdung und Schadenszustand zwei Aspekte, nämlich das Versagen von Abwehrmaßnahmen und das Bestehenbleiben von ungünstigen Umständen (/73/, Seite 85). Da nicht jede Gefährdung zwangsläufig zu einem Unfall führt, müssen also die Möglichkeiten der Gefahrenabwehr bewertet werden. Bei der Einschätzung der Gefahrenabwehr können folgende Fragen gestellt werden: „*Wenn eine gefährliche Situation eintritt,*

- *welche (menschlichen) Handlungen sind erforderlich, um einen Unfall zu verhindern?*
- *wie schnell muss der Mensch reagieren, um einen Unfall zu verhindern?*
- *welche Indikatoren/Hinweise würden den Menschen vor einer gefährlichen Situation warnen?*
- *bei einem technischen Ausfall, wie zuverlässig ist die Fehleranzeige – wird der Ausfall durch andere Systeme bestätigt?“ (aus dem Englischen nach /70/).*

Neben der betrieblichen Dauer der Gefährdung haben vor allem menschliche Handlungen und betriebliche Randbedingungen Einfluss auf die Gefahrenabwehr. Diese Gegebenheiten und Einflüsse müssen jedoch explizit außerhalb des definierten Systems liegen.

Wie in Kapitel 5.3.1 ausgeführt wurde, ist die Gefährdungsdauer entweder nicht relevant oder kann zur sicheren Seite abgeschätzt werden. Sie wird im Rahmen der Gefahrenabwehr nicht betrachtet. Die Wahrscheinlichkeit für die externen Risikoreduktionsfaktoren G_i eines Gefährdungsszenarios i kann somit nach folgender Beziehung abgeschätzt werden (siehe Gleichung 5-11):

$$G_i = B_i + M_i \quad \text{mit}$$

B_i = betriebliche Randbedingungen, ausgedrückt durch die mittlere Konfrontationswahrscheinlichkeit nach Hinzen (/73/). Dieser Wert sagt aus, wie wahrscheinlich es unter gegebenen betrieblichen Randbedingungen ist, dass sich im folgenden Abschnitt ein Zug befindet.

M_i = Möglichkeit der menschlichen Gefahrenabwehr, ausgedrückt durch die menschlichen Fehlerraten nach Hinzen³⁰ (/73/). Diese berücksichtigen menschliche Handlungen, die nicht dem System zugerechnet werden können bzw. nicht planmäßig erfolgen.

³⁰ Es gibt zahlreiche Untersuchungen zum Thema ‚Zuverlässigkeit des Menschen‘ (auch im Bereich Human Factors). Die Untersuchungen von Hinzen wurden hier zu Grunde gelegt, weil die verwendeten Wahrscheinlichkeiten in Rahmen der ‚üblichen‘ (in der Literatur vorkommenden) Größenordnungen liegen und sie zurzeit die einzigen quantitativen Werte speziell für den Bereich Eisenbahn darstellen. Nach Expertenschätzung wäre der Aufwand, um ‚bessere‘ (zuverlässigere) Werte für menschliche Fehlerwahrscheinlichkeiten zu erhalten sehr bzw. viel zu hoch.

6.1.1 Betriebliche Randbedingungen

Hinzen versteht unter Gefahrenfreiheit einen betrieblichen Zustand, „bei dem innerhalb zweier benachbarter Fahrwegabschnitte kein oder höchstens ein ungünstiger Umstand auftritt.“ (/73/, Seite 82). Für ungünstige Umstände im Eisenbahnbetrieb nennt er folgende Beispiele:

- Anwesenheit eines stehendes Fahrzeugs auf einem Fahrwegabschnitt, während auf dem benachbarten Fahrwegabschnitt eine Zug- oder Rangierfahrt stattfindet;
- Vorhandensein einer Weiche, die nur mit verminderter Geschwindigkeit befahren werden darf, in einem Fahrwegabschnitt, der befahren wird.

Grundlage für den Parameter b ist die Wahrscheinlichkeit für die Konfrontation von diesen ungünstigen Umständen. Als Schätzwert für die Konfrontationswahrscheinlichkeit von ungünstigen Umständen wird allerdings nur der mittlere Belegungsgrad des DB-Netzes pro Jahr herangezogen (Stand 1993). Bei der Berechnung gehen Parameter wie Betriebsleistung, mittlere Reisegeschwindigkeit, Anzahl der Signalzugfahrten, Sperr- und Belegungszeiten sowie die Anzahl von Signalabschnitten ein. Die mittlere Konfrontationswahrscheinlichkeit berechnet Hinzen zu $w_k = 0,0845$, die für die Anwendung in BP-Risk auf 0,1 (zur sicheren Seite) aufgerundet wird, um einen einfacheren Wert zu erhalten. Die Differenz von 0,1 zu 0,0845 würde sich nur als Konstante beim Rundungsfehler wiederfinden, die als Verschiebung des Skalennullpunktes herausfallen würde.

Die Konfrontationswahrscheinlichkeit von 0,1 wird im Rahmen von BP-Risk verstanden als folgende Aussage: ‚in 10% der Fälle befindet sich im nächsten Abschnitt ein Zug‘. Dies gilt für den Normalfall – also für eine durchschnittliche Betriebsdichte. Demzufolge wird dem quantitativen Wert $b = 10\%$ die qualitative Beschreibung ‚normal‘ zugewiesen (siehe Tabelle 6-2). Als erläuterndes Beispiel dienen Angaben zur Streckenkategorie. Als durchschnittlich wird hier eine Regionalverkehrsstrecke (R 120) angenommen, deren maximale Streckenauslastung laut DB-Richtlinie 413 (/37/) bei ca. 100 Zugpaaren pro Tag liegt (siehe Tabelle 6-3).

Tabelle 6-2 Skala für Parameter B

| b | log b | Rf | B | Qualitative Beschreibung | Beispiele |
|----------|--------------|-----------|----------|---------------------------------|--|
| 3,16 | 1,00 | 0,00 | 1 | Gering | Unter Netzdurchschnitt, z. B. auf Güterverkehrsstrecken |
| 10,00 | 2,00 | 0,00 | 2 | Normal | Netzdurchschnitt, z.B. auf Regionalverkehrsstrecke |
| 31,62 | 3,00 | 0,00 | 3 | Erhöht | Über Netzdurchschnitt, z. B. auf Fernverkehr- und HGV-Strecken |

b = Konfrontationswahrscheinlichkeit nach Hinzen (Wert in %)

Tabelle 6-3 Zusammenstellung der Streckenstandards (vereinfacht nach /37/)

| Streckenstandards | Leitgeschwindigkeitsstufen [km/h] | Optimierungskriterien | Streckenauslastung (Obergrenze) [Zp/d ³¹] |
|-------------------|-----------------------------------|---|---|
| P 300 (NBS) | 231 - 300 | HGV ³² | 120 |
| P und M 230 (ABS) | 161 - 230 | schneller SPFV ³³ , Mischverkehr | 150 |
| P und M 160 | 121 - 160 | schneller SPFV und SPNV, Mischverkehr | 150 |
| G und R 120 | 81 - 120 | Güterverkehr, SPNV | 100 |
| R 80 | 51 - 100 | SPNV ³⁴ | 25 |
| G 50 | 50 - 80 | regionaler SGV ³⁵ | 10 |

Im Rahmen der DB-Richtlinie 413 führten die Erkenntnisse aus den Planungen zu Neubaustrassen (NBS) und Ausbaustrecken (ABS) zur standardisierten Vorgabe von Infrastrukturparametern nach 10 Streckenstandards. Ausgehend von Leitgeschwindigkeit, Streckenauslastung und Entmischung der Verkehre unterschiedlicher Geschwindigkeiten bzw. Harmonisierung der Geschwindigkeiten stehen die Buchstaben in Tabelle 6-3 für:

- P = Personenverkehrsstrecke,
- M = Mischverkehrsstrecke,
- G = Güterverkehrsstrecke und
- R = Regionalverkehrsstrecke.

Ergänzend dazu geben die Zahlen 300, 230 usw. die Obergrenze der Leitgeschwindigkeitsstufen an. Die Leitgeschwindigkeit ist die, entsprechend der langfristigen Planung, vorgegebene und zu realisierende zukünftige Höchstgeschwindigkeit.

Da die Intervalle der Werte für die Streckenauslastungen (Zugpaare pro Tag) für die einzelnen Streckenstandards z. T. sehr groß sind und so eine Einschätzung nur grob möglich ist, werden für den Parameter B nur drei Klassen angenommen.

Alle quantitativen Werte für den Parameter *b* werden nach der oben genannten Anforderung so aufgestellt, dass der absolute Unterschied der Werte $\sqrt{10}$ entsprechen soll. Die zugehörigen qualitativen Beschreibungen und Beispiele orientieren sich an den Angaben aus den DB-Streckenstandards (siehe auch Anhang D: Streckenstandards). Dadurch wird gewährleistet, dass die Beispiele unabhängig von anderen Risikoparametern formuliert werden.

³¹ Zp/d: Zugpaare pro Tag.

³² HGV: HochGeschwindigkeitsVerkehr.

³³ SPFV: spurgeführter Personenfernverkehr.

³⁴ SPNV: spurgeführter Personennahverkehr.

³⁵ SGV: spurgeführter Güterverkehr.

Die Skalennullpunkte werden in Tabelle 6-2 nicht verschoben, da der transformierte Parameter B bereits bei ‚Eins‘ beginnt. Auf den Rundungsfehler muss hier keine Rücksicht genommen werden, weil er bei allen Werten Null beträgt.

Wichtig bei der Bewertung der Betriebsdichte ist, dass dieser Parameter unabhängig von der Geschwindigkeit betrachtet wird. Die Angaben der Verkehrsstrecken aus den Streckenstandards sind lediglich Beispiele für die Streckenauslastung und sollten nicht dazu verwendet werden, Rückschlüsse auf die gefahrene Geschwindigkeit zu ziehen. So können beispielsweise S-Bahnen, die zum spurgeführten Personennahverkehr (SPNV) gehören, durchaus eine erhöhte Betriebsdichte auf ihren Strecken haben, obwohl geringere Streckengeschwindigkeiten vorliegen.

6.1.2 Menschliche Gefahrenabwehr

Nach Hinzen erreicht das Mensch-Maschine-System den Schadenszustand nur dann, „*wenn sowohl der Mensch nicht zufällig eingreift als auch die physikalischen Gegebenheiten [...] nicht günstig sind*“ (/73/, Seite 201). Die physikalischen Gegebenheiten sind bei BP-Risk über den Parameter B bereits berücksichtigt worden. Das mögliche Eingreifen des Menschen soll nun im Parameter M bewertet werden. Nach Hinzen ist es jedoch „*sehr schwierig, Situationen, wie das zufällige Eingreifen eines Menschen zur Vermeidung eines Schadens datenmäßig zu erfassen*“ (/73/, Seite 202).

Grundsätzlich sollten bei Risikobeurteilungen jedoch der Mensch als Bediener oder Benutzer in die Analyse mit einbezogen werden. Allerdings ist sehr genau zu prüfen, ob der Mensch Teil des betrachteten Systems ist (was in der Regel der Fall ist). Die Quantifizierung der Verlässlichkeit menschlichen Verhaltens ist ein eigenständiges Gebiet (Human Factors). In diesem Bereich gibt es zahlreiche Diskussionen darüber, ob ein Mensch überhaupt in Form von Fehlerraten oder Fehlerwahrscheinlichkeiten ‚quantifiziert‘ werden kann. Deswegen sollten in der Regel nach /11/ für diesen Bereich nur moderate Annahmen gemacht werden. Das ist der Grund, warum im Rahmen von BP-Risk der M -Parameter ‚nur‘ drei Parameterwerte für den Anwender vorgibt.

Bei der Betrachtung dieses Parameters soll also bewertet werden, inwiefern der Mensch die Gefahr erkennen und den Schaden noch abwenden kann. An dieser Stelle soll nur der Eingriff des Menschen betrachtet werden, der durch seine Handlung eine Gefahr abwehren kann. So ist es z. B. denkbar, dass ein Triebfahrzeugführer (Tf), dem eine zu hohe Geschwindigkeit für eine abzweigende Weiche signalisiert wird, aufgrund seiner Streckenkenntnis die gefährliche Situation erkennt und die Geschwindigkeit noch rechtzeitig drosseln kann. Außerdem könnte es sein, dass ihm ein Abschnitt fälschlicherweise als frei signalisiert wird, der Tf jedoch die Gefahr (möglicherweise einen im Abschnitt stehenden Zug) erkennt und seinen Zug noch rechtzeitig anhalten kann (Beispiele nach /9/, Seite 104ff).

Ein weiterer Fall wäre, dass einem Fahrdienstleiter (Fdl) oder Tf im betrieblichen Ablauf eine Unstimmigkeit oder Besonderheit zufällig auffällt, der dann zum Beispiel über Zugfunk einen Nothaltauftrag erteilt und damit die drohende Betriebsgefahr abwendet (nach /73/, Seite 203).

Die hier in Frage kommenden menschlichen Handlungen finden in der Regel unter ungünstigen Umständen statt und werden bei kurzer Reaktionszeit unter Stress durchgeführt. Daher wird im Rahmen von BP-Risk nur eine menschliche Handlung bewertet (bei mehreren Auswahlmöglichkeiten sollte die Erfolgversprechendste berücksichtigt werden). Außerdem befindet sich der Mensch bei einem Funktionsversagen in einer Situation, in der er nicht mehr seine Routineaufgaben ausführt. Aus den genannten Gründen werden als Grundlage für den Parameter *M* die menschlichen Fehlerraten nach Hinzen nur für menschliche Handlungen unter ungünstigen Umweltbedingungen herangezogen (siehe Tabelle 6-4).

Tabelle 6-4 Menschliche Fehlerraten nach Hinzen (/73/, Seite 62)

| Menschliche Handlungen | Umweltbedingungen | Menschliche Fehlerrate <i>f</i> |
|------------------------|-------------------|---------------------------------|
| Fertigkeits-basierend | ungünstig | $1 \cdot 10^{-2}$ |
| Regel-basierend | ungünstig | $1 \cdot 10^{-1}$ |
| Wissens-basierend | ungünstig | 1,0 |

Für die Begriffe aus Tabelle 6-4 gelten folgende Definitionen:

„Fertigkeits-basierendes“ Verhalten ist dann gegeben, wenn der Mensch die ihm gestellte Aufgabe eindeutig verstanden hat und sie aufgrund seiner Ausbildung mit automatisch ablaufenden, sensomotorischen Reaktionen ausführen kann.

Regel-basierendes Verhalten ist dann gegeben, wenn der Mensch die ihm gestellte Aufgabe aufgrund festgelegter Symptome einer gelernten Sammlung von Verhaltensregeln der Form ‚Wenn - Dann‘ zuordnen und mit der so gefundenen Regel ausführen kann.

Wissens-basierendes Verhalten ist dann gegeben, wenn der Mensch die ihm gestellte Aufgabe aus Mangel an Erfahrung nur lösen kann, indem er seinen Wissensschatz über die Funktionsweise des Systems nutzt, um komplexe oder gar mehrdeutige Informationen auszuwerten, eine Entscheidung aufgrund allgemeiner Ziele zu treffen und dann zu handeln“. (/73/, Seite 62).

Der Anwender hat bei der Bewertung vom Parameter *M* zu entscheiden, um was für eine Kategorie von menschlichen Handlungen es sich handelt. Dabei ist zu beachten, dass die Bewertung von BP-Risk ein Gefährdungsszenario betrachtet, d. h. die Gefährdung liegt bereits vor. Es ist zu diskutieren, ob bei Vorhandensein einer gefährlichen Situation überhaupt noch ein fertigkeit-basierendes Verhalten des Menschen möglich ist. In der Regel sind Gefährdungen und dementsprechende menschliche Hilfshandlungen sehr selten und kaum trainiert – es liegen also keine routinemäßige Handlungen vor (siehe auch /112/). Es mag jedoch Ausnahmen geben, bei denen noch fertigkeit-basierende Handlungen selbst unter ungünstigen Umständen möglich sind, z. B. das Erkennen, ob eine Weiche falsch steht.

Diese Handlung nennt Hinzen (/73/) explizit in seiner Arbeit als Beispiel für fertigkeits-basierende menschliche Handlungen (siehe Aufzählung unten). Deswegen wird die menschliche Fehlerrate für fertigkeits-basierende Handlungen im Rahmen von BP-Risk mitberücksichtigt, allerdings nur unter ungünstigen Umweltbedingungen. Die Fehlerraten gelten pro menschliche Handlung, wobei der Begriff ‚Handlung‘ nicht definiert wird. Hinzen nennt jedoch einige Beispiele für fertigkeits- und regel-basierende Handlungen in seiner Arbeit³⁶:

Fertigkeits-basierende Handlungen:

- Fernmündliche Meldung,
- Fahrwegsicherung,
- Weichen stehen richtig,
- Tf fährt auf Sicht,
- Zuordnung von Signalen zu Gleisen und Bedeutung durch Tf,
- Streckenkenntnis des Tf über Besonderheiten,
- Anstandslose Bedienung der Sifa nur im Wachzustand,
- Bemerken und Beachten des Halt-zeigenden Signals,
- Fdl bietet Zug an und wiederholt Annahme,
- Nachbar-Fdl nimmt Zug an und bestätigt Richtigkeit.

Regel-basierende Handlungen:

- Zugschlussfeststellung,
- Signalhaltfeststellung,
- Fdl diktiert Befehl und bestätigt Richtigkeit,
- Tf schreibt Befehl und wiederholt Wortlaut,
- Fdl bietet falsch fahrenden Zug an und wiederholt Annahme,
- Nachbar Fdl nimmt falsch fahrenden Zug an, bestätigt Richtigkeit der Wiederholung.

Der Parameter *M* ist in Tabelle 6-5 zusammengefasst und berücksichtigt die bereits oben genannten Anforderungen an die Tabellenbeschreibung. Im Rahmen von BP-Risk wird eine menschliche Fehlerrate von $f = 1,0$ verstanden als ‚100% der Entscheidungen des Menschen sind falsch‘. So wird $m = 100\%$ qualitativ beschrieben als ‚Gefahrenabwehr fast nie möglich‘, da hier nur noch ein zufälliges Eingreifen des Menschen die Gefahr abwenden könnte. Die Fehlerraten für regel- bzw. fertigkeits-basierende menschliche Handlungen werden dementsprechend übertragen.

In Ausnahmefällen können nach /9/ (Seite 105) für die Bewertung des *M*-Parameters auch andere technische Systeme zum Tragen kommen, dabei ist dann aber immer zu prüfen, ob

- Unabhängigkeit zum betrachteten System vorliegt, oder
- ggf. wieder menschliche Handlungen eine Rolle spielen, oder
- die Gefahrenabwehr quasi automatisch unterstützt wird.

³⁶ Die Zuordnung der Handlungen ist unter Experten umstritten und dient hier lediglich als Beispiel.

Tabelle 6-5 Skala für Parameter M

| m | log m | Rf | M | Trans (M+1) | Qualitative Beschreibung | Beschreibung |
|--------|-------|------|---|----------------|-----------------------------|---|
| 1,00 | 0,00 | 0,00 | 0 | 1 | Häufig möglich | Fertigkeits-basierend unter un- günstigen Umständen |
| 10,00 | 2,00 | 0,00 | 2 | 3 | Selten möglich | Regel-basierend unter ungünsti- gen Umständen |
| 100,00 | 4,00 | 0,00 | 4 | 5 | Fast nie möglich | Zufälliges Eingreifen des Men- schen (Wissens-basierend) |

m = menschliche Fehlerrate nach Hinzen (Wert in %),

6.2 Schadensausmaß

Nach DIN EN ISO 14971³⁷ wird Schadensausmaß definiert als „*qualitatives Maß für die möglichen Folgen/Konsequenzen einer Gefährdung.*“ Schaden wird dort definiert als „*Verletzung von Körper, Gesundheit und/oder Leben (Personenschäden), Schädigung von Eigentum oder Vermögen (Sachschäden) und Umwelt (Umweltschäden)*“ (aus dem Englischen /41/).

Im Rahmen von Risikobeurteilungen wird oft der Personenschaden als Risikokenngröße verwendet. Es wird dabei angenommen: „*wenn das Transportgefäß (Fahrzeug) gesichert ist, ist die Sicherheit insgesamt gegeben*“ (/109/). Demnach wird auch bei BP-Risk davon ausgegangen, dass wenn der zu betrachtende Zug hinreichend geschützt ist, auch die anderen Rechtsgüter (wie Personen, Umwelt, Sachwerte, Image des Bahnbetreibers, etc.) hinreichend geschützt sind.

Bei der Bewertung des Schadens für den zu betrachtenden Zug soll nun eingeschätzt werden, welches Ausmaß der Personenschaden einnehmen könnte, falls auch die eventuell mögliche Gefahrenabwehr misslingt. Dies erfolgt nach Gleichung 5-12 durch die Ermittlung der drei Sub-Parameter für das jeweilige Gefährdungsszenario i :

$$S_i = T_i + V_i + A_i \quad \text{mit}$$

T_i = Masse, ausgedrückt durch die durchschnittlich maximale Last für die jeweilige Zuggattung. Die Zuggattungen werden klassifiziert entsprechend der DB-Streckenstandards.

V_i = maßgebliche Geschwindigkeit des zu betrachtenden Zuges, kategorisiert durch die erlaubte Geschwindigkeit auf bestimmten Strecken bzw. bei bestimmten Betriebsmodi.

A_i = Anzahl betroffener Personen, in Abhängigkeit der jeweiligen Unfallkategorie. Die Unfalltypen werden kategorisiert nach der EBA Anweisung für „Gefährliche Ereignisse im Eisenbahnbetrieb“.

³⁷ DIN EN ISO 14071: Internationale Norm zum Risikomanagement für Medizinprodukte.

6.2.1 Maximale Last

Die Grundlage für die Schadensbewertung bildet die kinetische Energie, die beim Unfall wirksam wird und die auf vom Unfall betroffenen Personen wirkt. Die kinetische Energie ist die Energie, die in der bewegten Masse eines Körpers enthalten ist. Sie hängt von der Masse und von der Geschwindigkeit des bewegten Körpers ab.

Bei BP-Risk wird die Masse durch den Parameter t und die Geschwindigkeit durch den Parameter v (siehe Kapitel 6.2.2) bewertet. Dabei wird für den Parameter t die Kategorisierung der Zugklassen aus der DB Richtlinie 413 (/37/) zu Grunde gelegt, um die verschiedenen Zuggattungen³⁸ und ihre Massen zu berücksichtigen.

Eine andere denkbare Möglichkeit, die Kritikalität eines Schadens in Abhängigkeit der Masse auszudrücken, wäre die Differenzierung nach Hindernissen, auf die der betrachtete Zug im Fall einer Kollision auftrifft (z. B. ein Prellbock mit geringer Masse oder ein anderer Zug mit großer Masse). Diese Einteilung würde jedoch zum einen nicht zum Modell der kinetischen Energie passen, da dort die Masse des *bewegten* Körpers betrachtet wird, und zum anderen wird davon ausgegangen, dass das Hindernis, auf das der Zug treffen könnte, zufällig ist. So ist eine Unterscheidung der Hindernisse nur bedingt und in einigen Fällen (z. B. bei einer Entgleisung) gar nicht möglich.

Die DB Richtlinie 413 definiert Zugklassen, die die Zielsetzung Netz 21³⁹ der Deutschen Bahn AG mit der Streckenstandardisierung hinreichend genau beschreiben. Diese Zugklassen können bei Bedarf auf das Trassenpreissystem transferiert werden. Die für die Zugpreisklassen beschriebenen Zugklassen und Zuggattungen enthalten Angaben zur maximalen Last, die dem Parameter t im Rahmen von BP-Risk zu Grunde gelegt werden. Diese Daten sind in Tabelle 6-6 vereinfacht zusammengefasst.

Tabelle 6-6 Zugpreisklassen (vereinfacht nach /37/)

| Zugklasse | Maximale Last [t] | Geschwindigkeit [km/h] | Zuggattung |
|-----------|-------------------|------------------------|--|
| HGV | 1000 | ≥ 200 | Triebzug |
| SPFV | 600 - 750 | 140 - 200 | Triebzug, bespannte Personenfernverkehrszüge, Nachtzüge, Autoreisezüge |
| SPNV | 400 - 500 | 120 - 140 | Regionalbahn (RB), Stadtexpress (SE), S-Bahn-Züge |
| SGV | 1300 - 2500 | 90 - 120 | Güterzüge (ohne Bedienung im Nahbereich) |

³⁸ Durch eine Buchstabenkennung ausgedrückte Bezeichnung zur Unterscheidung der Züge nach ihren Aufgaben (/95/).

³⁹ Name einer Strategie, mit der die DB AG versucht, die Leistungsfähigkeit ihres Vorrangstreckennetzes zu erhöhen.

Die maximale Last (in Tonnen) wird für die jeweilige Zuggattung errechnet, in dem die Durchschnittswerte für die Zugklassen SPNV, SPFV und HGV sowie SGV ermittelt werden. Angaben zum Mischverkehr werden in der Richtlinie nicht gemacht. In der Regel sind auf Mischverkehrstrecken jedoch die Anforderungen im Personenverkehr ausschlaggebend. Zur Vereinfachung werden SPFV und HGV zusammengefasst. Die gerundeten Durchschnittswerte bilden den Ausgangswert t der Tabelle 6-7.

Tabelle 6-7 Skala für Parameter T

| t | $\log t$ | R_f | T | Transf (T-4) | Qualitative Beschreibung | Beispiele |
|------|----------|-------|-----|--------------|--------------------------|--|
| 433 | 5,27 | -0,27 | 5 | 1 | SPNV | Regional Bahn, Stadtexpress, S-Bahn Züge |
| 775 | 5,78 | 0,22 | 6 | 2 | SPFV + HGV | Triebzüge, bespannte Personenverkehrszüge, |
| 1920 | 6,57 | 0,43 | 7 | 3 | SGV | Güterzüge (auch Schnellgüterzüge) |

t = durchschnittliche, maximale Last für jeweilige Zuggattung (Wert in Tonnen)

Die Skalennullpunkte werden entsprechend verschoben, so dass der transformierte Parameter T mit dem Wert ‚Eins‘ beginnt. Die qualitative Beschreibung der Zuggattungen sowie die Beispiele werden von den Streckenstandards aus /37/ übernommen.

Die hohe Gewichtung der Zuggattung Güterzüge in Tabelle 6-7 wirft die Frage auf, ob die Anforderungen für den Güterverkehr im Vergleich zum Personenverkehr nicht zu hoch bewertet werden. Allerdings bietet BP-Risk durch die Parameter Geschwindigkeit und Betriebsdichte die Möglichkeit diese Gewichtung auszugleichen. Denn im Güterverkehr ist mit geringeren Geschwindigkeiten und mit einer geringeren Betriebsdichte zu rechnen als im Personenverkehr, so dass die Anforderungen mindestens zwei Stufen geringer sind, was ungefähr einer Zehnerpotenz entspricht.

6.2.2 Maßgebliche Geschwindigkeit

Bei Unfällen des gleichen Typs können sehr starke Unterschiede bei den wirkenden Kräften auftreten. Diese sind in erster Linie von den gefahrenen Geschwindigkeiten abhängig. Zu beachten ist, dass bei der quadratischen Geschwindigkeit des Zuges v_i^2 nicht die Differenzgeschwindigkeit von z. B. zwei zusammenstoßenden Zügen, sondern im Rahmen von BP-Risk nur die maßgebliche Geschwindigkeit des zu betrachtenden Zuges berücksichtigt wird. Dabei ist weiterhin wichtig, dass die durchschnittlich auftretende Situation bewertet wird. ‚Worst-case‘-Annahmen würden hierbei zu falschen Ergebnissen führen.

Bei Risikobeurteilungen kommt häufig die Frage auf, ob die Geschwindigkeit wirklich einen quadratischen Einfluss auf den Unfallschaden hat und ob sich nicht eine Sättigung bei hohen Geschwindigkeiten einstellt.

Quadratischer Einfluss

Untersuchungen zur Abschätzung der Unfallschwere mit Hilfe von statistischen Auswertungen von Unfällen in Europa (/63/) ergaben, dass ein statistisch signifikanter Zusammenhang zwischen Unfallschwere und kinetischer Energie nur für Frontal-Zusammenstöße nachgewiesen werden konnte. Nach Expertenmeinung war es im Rahmen dieser Untersuchung jedoch nicht nachvollziehbar, warum sich nur bei Frontal-Zusammenstößen und nicht auch beispielsweise bei Auffahrten (Aufprall) ein statistisch signifikanter Zusammenhang ergab. Normalerweise würde man auch hier denselben Zusammenhang (allerdings mit kleinerer wirksamer Masse bzw. Geschwindigkeit) erwarten. Dieser Argumentation folgend wird für BP-Risk durchgängig die quadratische Geschwindigkeit als Grundlage für den Parameter v benutzt. Dies führt jedoch dazu, dass gerade die hohen Geschwindigkeiten eine starke Gewichtung bekommen und somit der gesamte V -Parameter eine starke Spreizung erfährt. Zum Vergleich der Spreizung des Schadensparameters siehe auch Kapitel 6.2.4.

Da bei langsamen Geschwindigkeiten das Quadrat von v noch nicht so stark wächst wie bei höheren Geschwindigkeitswerten, werden bei niedrigen Geschwindigkeiten mehr Werte zusammengefasst. So wird beispielsweise nicht explizit unterschieden zwischen den Geschwindigkeiten beim Rangieren (ca. 25 km/h), bei Fahrt auf Befehl (40 km/h z. B. für Zs1⁴⁰) oder auf Güterverkehrstrecken (Leitgeschwindigkeit 50 km/h), da diese geringen Geschwindigkeiten relativ nahe beieinander liegen. Als quantitativer Wert wird der Mittelwert für diese drei Geschwindigkeiten angenommen, der bei ca. 38 km/h liegt.

Sättigung

Untersuchungen zur Verteilung der Geschwindigkeiten bei Zusammenstößen und Zusammenprallen ergaben, dass die mittleren Geschwindigkeiten relativ gering sind (36, 55 bzw. 60 km/h nach /111/). Dies bedeutet, dass sich selbst bei hohen Streckengeschwindigkeiten eine gewisse Sättigung der Unfallgeschwindigkeit bei ca. 60 km/h ergibt. Diese Ergebnisse gelten allerdings für Zusammenstöße. Bei Entgleisungen sind immer noch höhere Geschwindigkeiten möglich (z. B. 120 km/h bei der Entgleisung eines japanischen Eilzugs nach /110/). Insbesondere auf Hochgeschwindigkeitsstrecken werden Weichen eingebaut, die im abzweigenden Gleis mit bis zu 160 km/h und mehr befahrbar sind. Somit wird bei BP-Risk eine Sättigung der Geschwindigkeiten bis 60 km/h angenommen, jedoch Geschwindigkeiten bis 160 km/h mitberücksichtigt. Um sowohl den möglichen Aspekt der Sättigung der Unfallschwere zu berücksichtigen als auch den Rundungsfehler klein zu halten, wird der Parameter V bei hohen Geschwindigkeiten jedoch nicht zu weit aufgefächert. So gibt es nur zwei Kategorien für Geschwindigkeiten ab 60 km/h.

⁴⁰ Das Ersatzsignal Zs1 ersetzt einen schriftlichen Befehl, der dem Tf gestattet an einem defekten oder gestörten Halt-zeigenden Hauptsignal vorbeizufahren. Es ordnet eine Geschwindigkeitsbeschränkung auf 40 km/h im möglicherweise folgenden Weichenbereich an, da dort Weichen auf Abzweig liegen könnten, die mit höchstens dieser Geschwindigkeit befahren werden dürfen. Wenn nicht zugleich Fahren auf Sicht angeordnet wird, darf nach dem Weichenbereich auf die zulässige Geschwindigkeit gemäß Fahrplan beschleunigt werden.

Um den qualitativen Beschreibungen Beispiele aus der Praxis zuzuordnen, werden für die quantitativen Werte die Leitgeschwindigkeiten der DB-Streckenstandards (/37/) herangezogen. So wird für Geschwindigkeiten zwischen 60 und 160 km/h der Mittelwert der Streckengeschwindigkeit für Nebenstrecken (Leitgeschwindigkeit 80 km/h) und Regionalstrecken (Leitgeschwindigkeit 120 km/h) angenommen, der bei 100 km/h liegt. Alle Werte und Beispiele für den Parameter V sind in Tabelle 6-8 zusammengefasst.

Tabelle 6-8 Skala für Parameter V

| v | $\log v^2$ | R_f | V | Trans (V-5) | Qualitative Beschreibung | Beispiele |
|-----|------------|-------|-----|----------------|-----------------------------|---|
| 38 | 6,30 | -0,30 | 6 | 1 | Gering | Rangieren, Fahrt auf Befehl ⁴¹ , Güterverkehrsstrecken (G50) |
| 60 | 7,11 | -0,11 | 7 | 2 | Mittel | Nebenstrecken (R80) |
| 100 | 8,00 | 0,00 | 8 | 3 | Hoch | Regionalstrecken (R120) |
| 160 | 8,82 | 0,18 | 9 | 4 | Sehr Hoch | Hauptstrecken (P160-230) und HGV-Strecken (P300) |

v = mittlere Geschwindigkeit (Wert in km/h)

6.2.3 Betroffene Personen

Bei der Bewertung der Anzahl der betroffenen Personen ist für den Anwender die Frage zu beantworten, welche typische Folge das betrachtete Gefährdungsszenario hat. Da es im Rahmen einer Folgenanalyse sehr schwierig ist, die Anzahl von Toten oder Verletzten direkt (sowohl quantitativ als auch qualitativ) zu schätzen, wird beim Parameter A die mittlere Anzahl der betroffenen Personen in Abhängigkeit des Unfalltyps angegeben.

In der EN 50129 ist Unfall definiert als „*ein nicht beabsichtigtes Ereignis oder eine Reihe von Ereignissen mit der Folge von Toten, von Verletzten, des Verlustes eines Systems oder von Umweltschäden*“ (/30/). Ähnlich beschreibt die DIN 13050 (Norm aus dem Rettungswesen) einen Unfall: „*ein plötzliches, unvorhergesehenes und durch äußere Ursachen eintretendes Ereignis, das zu einem Schaden an Personen und/oder Sachen führt*“ (/42/). Nach Europäischer Verordnung ist ein ‚schwerer Unfall‘: „*jeder Unfall, an dem mindestens ein in Bewegung befindliches Eisenbahnfahrzeug beteiligt ist und bei dem mindestens eine Person schwer verletzt oder getötet wird oder der erhebliche Sachschäden am Fahrzeugbestand, an den Gleisen, an anderen Anlagen bzw. in der Umgebung oder eine beträchtliche Störung des Verkehrs zur Folge hat. Unfälle in Werkstätten, Vorratslagern, Betriebswerken sind ausgenommen*“ (/50/).

⁴¹ In der Fahrdienstvorschrift KoRil 408 ist festgelegt, in welchen Fällen mit welchem Befehl ein Auftrag oder Hinweis übergeben werden muss und mit welcher Geschwindigkeit gefahren werden darf.

Von Unfällen spricht man also, wenn es zu Personenschäden und/oder zu Sachschäden kommt. Unfälle mit Zügen werden typischerweise nach ihrer Art unterschieden. Dazu werden in der Eisenbahn Bundesamt (EBA) Anweisung A 21, Unfälle⁴² unterteilt in:

- „Aufprall: Fahren gegen Personen (nicht Reisende) oder Hindernis im Regellichtraum (kein Arbeitsunfall).
- Entgleisung: Abgleiten oder Abheben eines Eisenbahnfahrzeugs von der Fahrbahn.
- Gefährliches Ereignis mit Reisenden: jedes Ereignis, bei dem Reisende konkret gefährdet oder geschädigt werden (Ausnahme: Suizide und Arbeitsunfälle).
- Zusammenprall: Zusammentreffen eines Eisenbahnfahrzeugs und eines Straßenverkehrsteilnehmers auf einem Bahnübergang (BÜ).
- Zusammenstoß: Zusammentreffen zweier Eisenbahnfahrzeuge durch z. B. Folgefahrt, Gegenfahrt, Flankenfahrt“ (/56/).

Diese Einteilung der Zugunfälle wird im Rahmen von BP-Risk für die Beschreibung des Parameters A verwendet. Nach obiger Annahme: „wenn das Transportgefäß (Fahrzeug) gesichert ist, ist die Sicherheit insgesamt gegeben“ (/109/), werden allerdings nur diejenigen Zugunfälle betrachtet, die das Schienenfahrzeug betreffen. Damit wird der Unfalltyp ‚Gefährliches Ereignis mit Reisenden‘ vorerst nicht betrachtet. Allerdings wird im Rahmen einer möglichen Erweiterung von BP-Risk in Kapitel 11 auf den Aspekt der Reisendensicherung noch einmal näher eingegangen.

Für den Anwender ist es wesentlich einfacher, eine Unfallkategorie wie Zusammenstoß oder Entgleisung einzuschätzen, als anzugeben, ob es wenige oder viele Tote bzw. Verletzte gibt. Im veröffentlichten Ansatz von BP-Risk (/9/, Seite 97ff) wurde noch zwischen dem Unfalltyp und der Anzahl betroffener Personen unterschieden. Es zeigte sich jedoch, dass diese beiden Parameter oft in Abhängigkeit voneinander formuliert wurden. So wurde beispielsweise die Einschätzung ‚sehr viele Personen sind betroffen‘ mit dem erwarteten Unfalltyp ‚Zusammenstoß‘ begründet. Da grundsätzlich die Risikoparameter unabhängig voneinander sein müssen, wurden nun diese beiden Aspekte ‚Unfalltyp‘ und ‚betroffene Personen‘ in einem Parameter (A) zusammengefasst.

Als Grundlage zur Beschreibung der Anzahl der betroffenen Personen dient der mittlere Personenschaden nach einer Auswertung der Unfallstatistik der DB AG in den Jahren 1989-1999 (siehe /109/). Die verschiedenen Körperschäden wie Tod, schwere oder leichte Verletzung, die bei einem Unfall auftreten können, wurden im Rahmen dieser Auswertung zu einer gemeinsamen Schadensgröße (Einheit: Unfallopfer) wie folgt zusammengefasst:

$$\text{Personenschaden} = \text{AnzahlTote} + (\text{AnzahlSchwerverletzte} / 10) + (\text{AnzahlLeichtverletzte} / 100)$$

⁴² Unfälle werden in der Anweisung A 21 „gefährliche Ereignisse – Kategorie 1“ genannt.

Diese Heuristik wurde schon häufig verwendet, um Unfallfolgen quantitativ ins Verhältnis zu setzen und um das Schadenspotential vergleichbar zu machen. Dieser Ansatz wurde auch schon in, vom EBA genehmigten, Risikoanalysen verwendet und wird auch aktuell von der ERA verfolgt (/18/).

Der mittlere Personenschaden ist im Rahmen der genannten Auswertung für verschiedene Personengruppen ermittelt worden, nämlich für Reisende, Mitarbeiter und Dritte. Reisende sind nach EBA Anweisung 21 definiert als *„alle Nutzer von Eisenbahnfahrzeugen oder Bahnsteiganlagen (einschließlich Zu- und Abgänge), ausgenommen Mitarbeiter der Eisenbahnunternehmen im Dienst“* (/56/). Die Werte der DB-Statistik gelten für alle drei Personengruppen, inklusive ‚Dritte‘. Dies führt unter anderem dazu, dass ein Zusammenprall ungefähr dieselbe Schadenshöhe hat wie ein Zusammenstoß. Wenn also die Personengruppe ‚Dritte‘ für den Parameter A mit betrachtet wird, bekommt der Unfalltyp ‚Zusammenprall‘ eine sehr starke Gewichtung, denn unter ‚Dritte‘ fallen beispielsweise die Straßenverkehrsteilnehmer am Bahnübergang. Bei Unfällen an Bahnübergängen kommen in der Regel die beteiligten Straßenverkehrsteilnehmer sowie der Tf ernsthaft zu Schaden (siehe auch Tabelle 6-9). Unfälle mit vielen Opfern bilden die Ausnahme.

Tabelle 6-9 Unfälle an Bahnübergängen und Personenschäden im Jahr 2006 (/34/)

| | Reisende | Beschäftigte der DB AG | Straßenverkehrsteilnehmer, Bahnfremde | Gesamt |
|------------------------|----------|------------------------|---------------------------------------|--------|
| Getötet | 0 | 0 | 55 | 55 |
| Schwer verletzt | 0 | 6 | 40 | 46 |
| Leicht verletzt | 45 | 55 | 74 | 174 |
| Gesamt | 45 | 61 | 169 | 275 |

Bahnübergänge sind nur auf Eisenbahnstrecken mit einer zulässigen Höchstgeschwindigkeit bis 160 km/h erlaubt. Im Gegensatz dazu können Zusammenstöße auch bei Geschwindigkeiten > 160 km/h stattfinden. Nach EBA - Definition sind immer zwei Züge an einem Zusammenstoß beteiligt, was bedeutet, dass bei einem Unfall mit Personenzügen mehrere Wagen betroffen sein können. Demnach sollte ein Zusammenstoß im Rahmen der Bewertung des Personenschadens stärker gewichtet werden als ein Zusammenprall, da beim Zusammenstoß mehr Unfallopfer möglich sind. Für den Parameter A wird folglich der mittlere Personenschaden nur für die Personengruppen ‚Reisende und Mitarbeiter‘ betrachtet, da sich damit eine realistischere Gewichtung der Unfalltypen ergibt (siehe Tabelle 6-10). Dies entspricht auch der Modellsicht des zu Grunde gelegten Risikomodells von BP-Risk, dass nur die Personen im betrachteten Zug berücksichtigt werden.

Tabelle 6-10: Personenschäden bei Zugfahrten

| Unfallart | Personenschaden je Unfall [Reisende und Mitarbeiter] |
|----------------------------|---|
| Aufprall (zusammengefasst) | 0,001 |
| Zusammenprall | 0,005 |
| Entgleisung | 0,014 |
| Zusammenstoß | 0,157 |

Diese Gewichtung aus Tabelle 6-10 wird für die Beschreibung der Anzahl der betroffenen Personen im Rahmen von Parameter A übernommen. Die resultierenden Werte sind in Tabelle 6-11 zusammengefasst.

Tabelle 6-11 Skala für Parameter A

| a | log a | Rf | A | Trans (A+1) | Qualitative Beschreibung | Beispiele |
|-----|-------|------|---|----------------|-----------------------------|---|
| 1 | 0,00 | 0,00 | 0 | 1 | Einzelne Person | Bei einem Aufprall oder im Güterverkehr |
| 3 | 0,95 | 0,05 | 1 | 2 | Wenige Personen | Bei einem Zusammenprall |
| 10 | 2,00 | 0,00 | 2 | 3 | Einige Personen | Bei einer Entgleisung |
| 30 | 2,95 | 0,05 | 3 | 4 | Viele Personen | |
| 100 | 4,00 | 0,00 | 4 | 5 | Sehr viele Personen | Bei einem Zusammenstoß |

a = Anzahl betroffener Personen (Reisende und Mitarbeiter in Abhängigkeit des Unfalltyps)

Die Bewertung der Personenschäden in Abhängigkeit des Unfalltyps berücksichtigt vorerst nicht die Besetzung der Züge. Detaillierte Betrachtungen werden zur Erhaltung der Einfachheit des Verfahrens erst einmal nicht weiter untersucht. Es wird jedoch in Kapitel 11 eine mögliche Erweiterung für BP-Risk in diesem Bereich diskutiert.

6.2.4 Exkurs: Bandbreite von S

Die folgende Betrachtung soll allein dazu dienen, eine realistische Spreizung (Anzahl der Zehnerpotenzen) des Schadensparameters beurteilen und sie mit der Spreizung des später konstruierten BP-Risk Schadensparameters (in Kapitel 6.2) vergleichen zu können. Um die Spannweite des S-Parameters zu diskutieren, wird hier ein Beispiel für eine Schadensbewertung in Anlehnung an /18/ gegeben. Dort wird eine quantitative Einordnung des Schadenspotenzials anhand der Beschreibungen der Gefahrenstufen der EN 50126 durchgeführt (siehe Tabelle 6-12).

Tabelle 6-12 Schadenspotenzial in Anlehnung an /18/

| Schaden | Beschreibung | EN 50126 | S' |
|--------------------|---------------------------------|--------------|----|
| 10^2 | (Eschede-Unfall ⁴³) | Katastrophal | 10 |
| 3×10^1 | Sehr viele Unfallopfer | | 9 |
| 10^1 | Viele Unfallopfer | | 8 |
| 3×10^0 | Mehrere Unfallopfer | | 7 |
| 10^0 | Einzelnes Unfallopfer | Kritisch | 6 |
| 3×10^{-1} | Mehrere Schwerverletzte | | 5 |
| 1×10^{-1} | Ein Schwerverletzter | | 4 |
| 3×10^{-2} | Mehrere Leichtverletzte | Marginal | 3 |
| 1×10^{-2} | Ein Leichtverletzter | | 2 |
| 0 | Keine Verletzten | Unbedeutend | 1 |

Dazu wurde der Ansatz aus Kapitel 6.2.3 zur quantitativen Bewertung von Unfallfolgen verwendet:

$$\text{Schaden}^{44} = \text{Anzahl Unfallopfer}^{45} + \text{Anzahl Schwerverletzte}^{46}/10 + \text{Anzahl Leichtverletzte}/100$$

Die Berechnung des Vergleichsparameters S' erfolgt nach der gleichen mathematischen Transformation wie bei BP-Risk (Logarithmus zur Basis $\sqrt{10}$, ganzzahliger Rundung und Verschiebung). Insgesamt ergibt sich eine Spreizung der qualitativen Beschreibung in Anlehnung an die Gefahrenstufen aus der EN 50126 von vier bis fünf Zehnerpotenzen (wenn man eine Basis von $\sqrt{10}$ zu Grunde legt). Diese Spannweite findet sich auch bei anderen Schadensbewertungstabellen, z. B. bei den RPZ (/17/) wieder. Die Ordinalskalen reichen typischerweise ebenfalls von 1 bis 10. Folglich sollte der BP-Risk Schadensparameter so konstruiert sein, dass er ungefähr fünf Zehnerpotenzen abdeckt. Der konstruierte S-Parameter von BP-Risk hat durch die Kombinationen der drei Subparameter T , V und A den Wertebereich $W(S) = [3, 4, \dots, 12]$ und deckt somit vier bis fünf Zehnerpotenzen ab, wenn die Grundlage der Logarithmus zur Basis $\sqrt{10}$ ist. Tabelle 6-13 stellt die Angaben aus Tabelle 6-12 (Vergleichswert S') dem Schadensparameter aus BP-Risk (Parameter S) gegenüber und zeigt, dass beide Schadensparameter dieselbe Spreizung haben.

⁴³ Der ICE-Unfall von Eschede war ein Zugunglück am 3. Juni 1998. Bei der Entgleisung kamen 101 Menschen ums Leben, 88 wurden schwer verletzt. Es war bis dahin das schwerste Zugunglück in der Geschichte der Deutschen Bahn sowie aller Hochgeschwindigkeitszüge weltweit.

⁴⁴ Personenschäden sind nach DIN 14971 definiert als „Verletzung von Körper, Gesundheit und/oder Leben“ (/41/).

⁴⁵ ‚Getötete‘ definiert die EG-Verordnung 91 als „alle Personen, die entweder unmittelbar nach einem Unfall oder innerhalb von 30 Tagen an den Unfallfolgen sterben – mit Ausnahme der Personen, die Selbstmord begangen haben“ (/50/).

⁴⁶ ‚Schwerverletzte‘ werden in der EG-Verordnung 91 definiert als „alle Verletzten, die nach einem Unfall für mehr als 24 Stunden in ein Krankenhaus eingewiesen wurden – mit Ausnahme der Personen, die einen Selbstmordversuch unternommen haben“ (/50/).

Der bereits veröffentlichte Ansatz aus (/9/, Seite 97ff) hat eine größere Spannweite für den Schadensparameter. Dort beträgt der Wertebereich $W(S) = [3, 4, \dots, 16]$, der somit sechs bis sieben Zehnerpotenzen abdeckt. Diese große Spreizung wird vor allem durch die starke Gewichtung der hohen Geschwindigkeiten und allgemein durch die detailliertere Auffächerung des Subparameters V verursacht.

Tabelle 6-13 Vergleichstabelle zur Spreizung von S

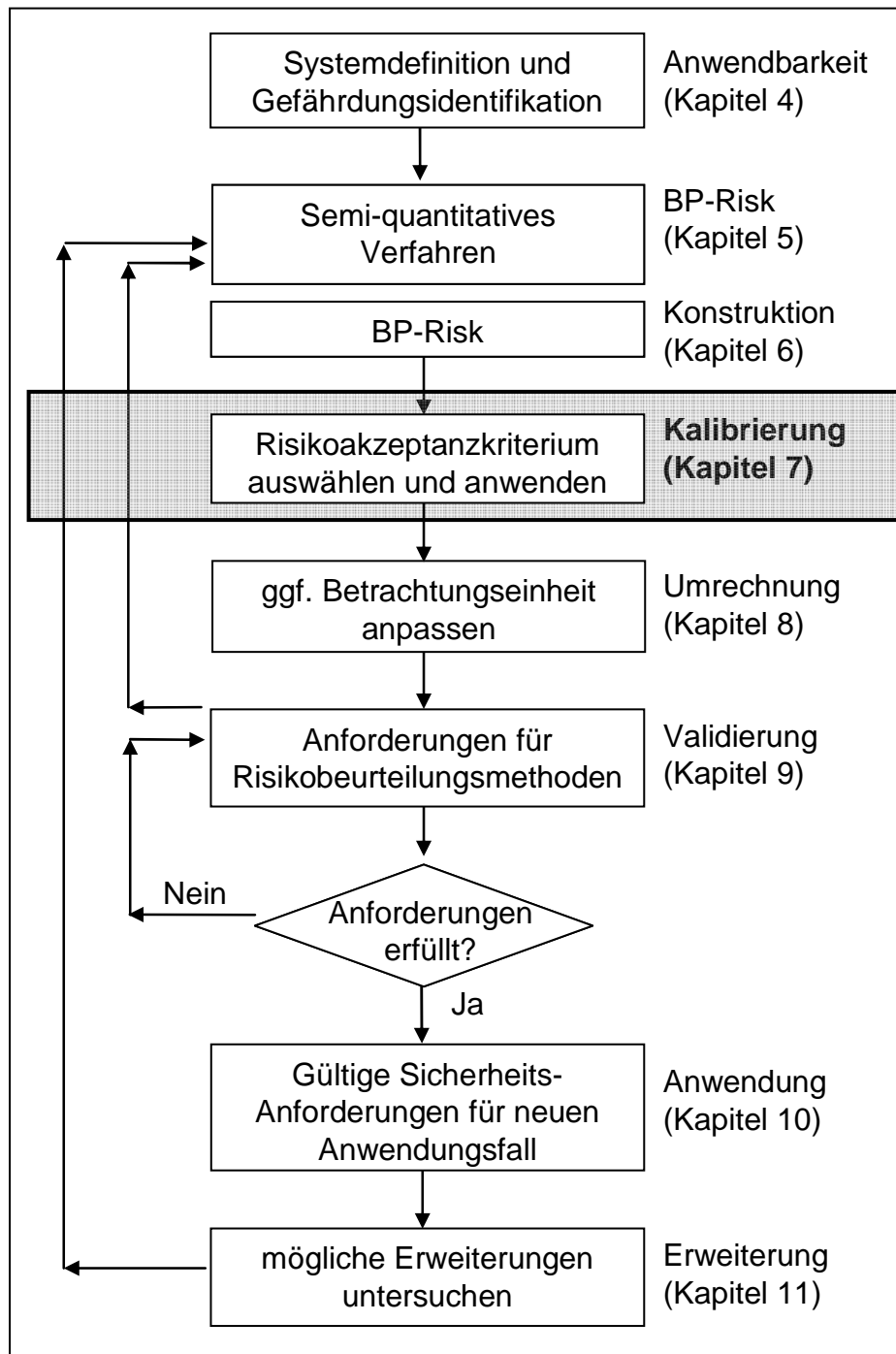
| Schaden | Beschreibung | EN 50126 | S' | S |
|--------------------|-------------------------|--------------|----|----|
| 10^2 | (Eschede-Unfall) | Katastrophal | 10 | 12 |
| 3×10^1 | Sehr viele Unfallopfer | | 9 | 11 |
| 10^1 | Viele Unfallopfer | | 8 | 10 |
| 3×10^0 | Mehrere Unfallopfer | | 7 | 9 |
| 10^0 | Einzelnes Unfallopfer | Kritisch | 6 | 8 |
| 3×10^{-1} | Mehrere Schwerverletzte | | 5 | 7 |
| 1×10^{-1} | Ein Schwerverletzter | | 4 | 6 |
| 3×10^{-2} | Mehrere Leichtverletzte | Marginal | 3 | 5 |
| 1×10^{-2} | Ein Leichtverletzter | | 2 | 4 |
| 0 | Keine Verletzten | Unbedeutend | 1 | 3 |

6.3 Zusammenfassung

BP-Risk stellt zum Thema Risikobeurteilung ein ‚best practice‘ dar, also ein aufgrund von Anforderungen optimales Verfahren. Die Methode ist nach europäischen Anforderungen für Risikobeurteilungen konstruiert und ermöglicht somit eine effiziente und anwenderfreundliche Durchführung der Ableitung von zulässigen Versagenshäufigkeiten der Funktionen eines Mensch-Maschine-Systems.

Beim grundlegenden BP-Risk Ansatz wurde in Kapitel 5 zunächst ein probabilistisches Risikomodell definiert, das das Risiko für ein Funktionsversagen in Abhängigkeit von Häufigkeit, Gefahrenabwehr und Schadensausmaß der betrachteten Systemgefährdung formuliert. Das probabilistische Modell wurde dann mittels einer mathematischen Transformation auf ein qualitatives Modell abgebildet, indem die quantitativen Risikoparameter diskretisiert und auf Parameterbereiche in Form von Tabellen abgebildet wurden. Dies erfolgte für alle Subparameter der Risikoparameter Gefahrenabwehr und Schadensausmaß in Kapitel 6. Zusätzlich erfolgte in Kapitel 6 die verbale Beschreibung der Tabellen anhand von eisenbahntechnischen Begriffen aus der betrieblichen Praxis.

Zur Herleitung der Tabelle für die zugehörige Gefährdungshäufigkeit muss das BP-Risk Verfahren anhand eines Risikoakzeptanzkriteriums kalibriert werden. Diese Kalibrierung und die Ableitung der Häufigkeitstabelle wird im folgenden Kapitel 7 beschrieben.



7 Kalibrierung

Bei einer Kalibrierung werden üblicherweise Messgeräte auf ein Richtmaß genormt. Kalibrieren umfasst die Ermittlung des Zusammenhangs zwischen den ausgegebenen Werten und den bekannten Werten der Messgröße unter bekannten Bedingungen. Bei der Kalibrierung wird BP-Risk auf ein gültiges Sicherheitsniveau eingestellt. Dazu wird ein europäisches Risikoakzeptanzkriterium als Kalibrierungspunkt implementiert und alle abhängigen Werte daran ausgerichtet. Das Risikoakzeptanzkriterium gibt somit die bekannten Werte und Bedingungen vor. Die ERA definiert ‚Risikoakzeptanzkriterium‘ als ein Bezugskriterium, „auf deren Grundlage die Vertretbarkeit eines Risikos bewertet wird“ (/59/).

7.1 Europäisches Risikoakzeptanzkriterium

Auf europäischer Ebene werden gemeinsame Sicherheitsziele (CST) angestrebt, um ein einheitliches Sicherheitsniveau für die Eisenbahn festzulegen. „Der Begriff des Risikoakzeptanzkriteriums wurde [jedoch] in der Vergangenheit stark strapaziert. Es wurde unisono immer wieder Klage geführt, dass alle Bemühungen daran scheitern, dass es in Europa kein einheitliches Risikoakzeptanzkriterium gäbe“ (/104/). Nach /16/ kommt die European Railway Agency (ERA) ebenso zum Schluss, dass eine übergreifende Abwärtsaufteilung von Sicherheitszielen auf Basis der CST nicht möglich ist. Daher hat sich der Verband der europäischen Eisenbahnindustrie (UNIFE) auf ein Kriterium für technische Systeme geeinigt. Dieses Risikoakzeptanzkriterium wird in der Empfehlung für gemeinsame Sicherheitsmethoden (CSM Recommendation) genannt. Es ist nur anzuwenden, wenn keine Verfahrensregeln („code of practice“) oder ähnliche Referenzsysteme („similar reference system“) vorhanden sind. Insofern passt es in den Scope von BP-Risk als Methode für die explizite Risikoeinschätzung („explicit risk estimation“) im Rahmen des ERA-Prozesses (siehe Abbildung 7-1).

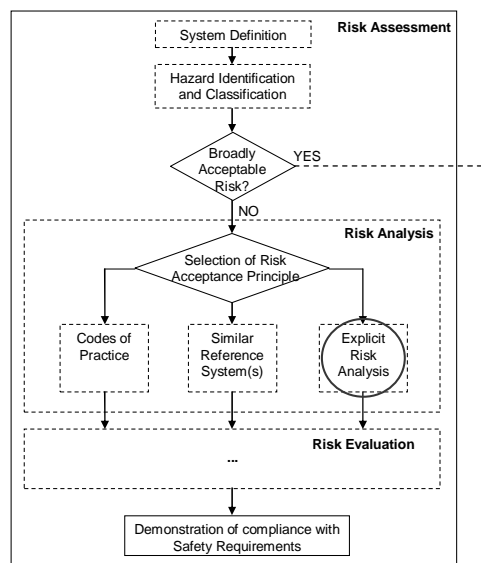


Abbildung 7-1 Anwendungsbereich von BP-Risk im Rahmen des ERA-Prozesses

Das Risikoakzeptanzkriterium für technische Systeme bei den europäischen Bahnen (RAC-TS) lautet: „Für technische Systeme in denen ein funktionales Versagen ein vorstellbares, direktes Potenzial für eine katastrophale Auswirkung hat, muss das assoziierte Risiko nicht weiter reduziert werden, wenn die Versagensrate kleiner oder gleich 10^{-9} pro Betriebsstunde beträgt“ (aus dem Englischen nach /62/, Artikel 10). Dabei wird ‚katastrophale Auswirkung‘ (oder Schaden) in Anlehnung an die EN 50126 definiert als „Unfalltote und/oder Schwerverletzte und/oder Umweltschäden“ (/28/). ‚Vorstellbares (oder glaubwürdiges) Potenzial‘ bedeutet: es ist wahrscheinlich, dass das jeweilige Funktionsversagen zu einem Unfall mit katastrophalen Schäden führt. Oder anders ausgedrückt, die Eintrittswahrscheinlichkeit eines Unfalls, der aus einer zugehörigen Gefährdung resultiert, ist nicht vernachlässigbar. ‚Direktes (oder unmittelbares) Potenzial‘ bedeutet in diesem Zusammenhang, dass es keine oder nur wenige Barrieren gibt, die bei einem Funktionsversagen einen Unfall verhindern könnten. Die Einheit ‚Betriebsstunde‘ bezieht sich direkt auf die Funktion, die zu einem Ausfall geführt hat. Wenn die Funktion z. B. fahrzeugseitig wäre, dann würde diese Einheit sich direkt auf eine Stunde des Zugbetriebs beziehen. Bei einer streckenseitigen Funktion wäre die Bezugseinheit ein Streckenelement, was folglich eine Anpassung der Betrachtungsgröße nötig machen würde (siehe dazu auch Kapitel 8).

Für technische Systeme ist eine Versagensart ein besonderer Fall einer Gefährdung. Während jedoch die übliche Definition von ‚Gefährdung‘ sehr weit gefasst wird, ist der Begriff ‚Versagensart‘ präziser und wird deshalb bevorzugt (/16/). Eine Versagensart entspricht beispielsweise im Rahmen einer FMEA (siehe Kapitel 4.3) einem Ausfallmodus einer Funktion. Die Funktionen, die auf dieses Kriterium angewendet werden sollen, müssen sich auf einer ähnlichen Funktionsebene befinden, z. B. Systemfunktionen eines Zuges (siehe Kapitel 4.2). RAC-TS wurde in Anlehnung an den Risikozielwert aus der Luftfahrt (siehe Abbildung 7-2) sowie aus der TSI-CCS⁴⁷ für ETCS⁴⁸-Fahrzeug- und Streckenausrüstung formuliert: „Für den sicherheitsrelevanten Teil der Fahrzeugausrüstung ergibt sich, ebenso wie für den sicherheitsrelevanten Teil der Streckenausrüstung, die geforderte Sicherheit für ETCS-Stufe 2 als: zulässige Gefährdungsrate von 10^{-9} pro Stunde [...]“ (/49/).

| von FHA ⁴⁹ abgeleitet | Sicherheitsziele |
|-------------------------------------|--|
| Versagenszustand Klassifikation | Quantitative Anforderung [pro Flugstunde] |
| Katastrophal | $< 10^{-9}$ |
| Schwerwiegend gefährlich | $< 10^{-7}$ |
| Bedeutend gefährlich | $< 10^{-5}$ |
| Geringfügig gefährlich | keine |
| Keine Auswirkung auf die Sicherheit | keine |

Abbildung 7-2 Sicherheitsziel der Luftfahrt (aus dem Englischen nach /106/)

⁴⁷ TSI-CCS-HS: TSI für Zugsteuerung, Zugsicherung und Signalgebung im HGV.

⁴⁸ ETCS: European Train Control System (europäisches Zugsicherungssystem).

⁴⁹ FHA: Functional Hazard Analysis (Funktionale Gefährdungsanalyse - Verfahren aus der Luftfahrt).

Nach /16/ ist das Ziel von RAC-TS, einen Referenzpunkt zu definieren, mit dem Risikoanalysen kalibriert werden können. Abbildung 7-3 zeigt die nötigen Kalibrierungsschritte am Beispiel der Risikomatrix aus der EN 50126:

- Der RAC-TS Referenzpunkt wird als tolerierbar eingestuft. Punkte mit einer höheren Häufigkeit oder Gefahrenstufe als RAC-TS werden als nicht tolerierbar klassifiziert.
- Die Abwägungsmechanismen („*Trade-off*“) der jeweiligen Methode wird dazu benutzt, um die Risikotolerierbarkeit auf nicht-katastrophale Ereignisse anzuwenden (z. B. durch Anwendung einer linearen Extrapolation mit dann festzulegender Steigung).

| Unfallhäufigkeit | Risikomatrix | | | |
|------------------|----------------------------|----------|----------|---------------|
| häufig | | | | |
| wahrscheinlich | | | | |
| gelegentlich | | | | |
| selten | | | | |
| unwahrscheinlich | | | | |
| unvorstellbar | | | | RAC-TS |
| | unbedeutend | marginal | kritisch | katastrophal |
| | Schwere des Unfalls | | | |

| | |
|--|---------------------|
| | = tolerierbar |
| | = nicht tolerierbar |

Abbildung 7-3 Kalibrierung einer Risikomatrix mit RAC-TS (in Anlehnung an /14/)

7.2 Kalibrierung

Um die zulässige Versagenhäufigkeit f z. B. in Form einer tolerierbaren Gefährdungsrate (THR) für die jeweilige Summe aus den Parametern Gefahrenabwehr und Schadensausmaß ($G+S$) abzulesen, wird die BP-Risk-Häufigkeitstabelle mit dem gewählten Risikoakzeptanzkriterium kalibriert. Dazu wird der Kritikalitätswert K für den Risikoakzeptanzwert berechnet, indem für ein gültiges Gefährdungsszenario i_T eine tolerierbare Gefährdungsrate F_T vorgegeben wird. Da RAC-TS als Kalibrierungspunkt in BP-Risk implementiert werden soll, wird hier $f_T = 10^{-9}/h$ gesetzt. Mit Hilfe der Berechnung von G_T und S_T für das zugehörige Gefährdungsszenario i_T erhält man die tolerierbare Kritikalität K_T (siehe Gleichung 7-1):

$$K_T = F_T + G_T + S_T \quad \text{Gleichung 7-1}$$

Für alle Gefährdungen, die sich auf der Ebene des tolerierbaren Gefährdungsszenarios i_T befinden, wird der Kritikalitätswert K_T als konstanter, akzeptierter Risikowert angenommen. Dieser Wert ist implizit in der BP-Risk Häufigkeitstabelle enthalten und wird nicht explizit ausgewiesen. Für ein beliebiges Gefährdungsszenario i (auf der korrekten Ebene) wird dann eine vereinfachte Folgen- und Konsequenzanalyse durchgeführt, indem die Parameter Gefahrenabwehr G_i und Schadenspotenzial S_i für die jeweilige Gefährdung H_i bewertet werden.

Im Rahmen von BP-Risk kann dann die zulässige Versagenhäufigkeit $F_i (\log_{10}(f_i))$ für beliebige Funktionsversagen mit Hilfe von Gleichung 7-2 berechnet werden:

$$F_i = K_T - (G_i + S_i) \quad \text{Gleichung 7-2}$$

Abbildung 7-4 illustriert das zugrunde liegende Prinzip in Anlehnung an den ‚Sanduhr-Prozess‘ aus Kapitel 2.2.2.

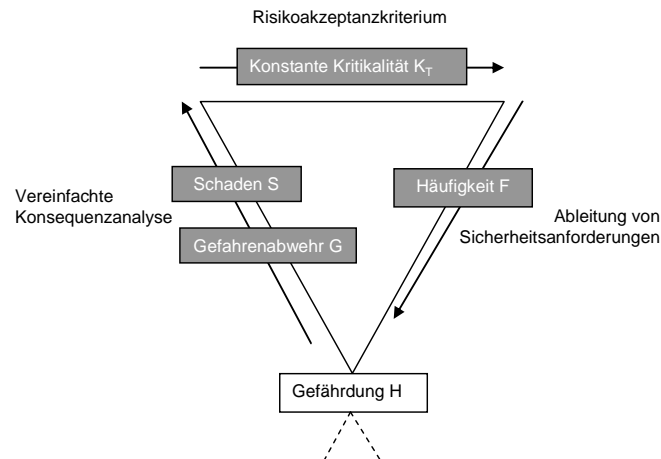


Abbildung 7-4 BP-Risk Prinzip

7.2.1 Gefährdungsszenario i_T

RAC-TS erfordert eine genaue Beschreibung der Funktionsebene, auf die das Risikoakzeptanzkriterium angewendet werden soll, denn es gibt „nur sehr wenige Versagensarten bei Funktionen, für die die Sicherheitsanforderungen direkt vom RAC-TS abgeleitet werden könnten, z. B.:

- Vollständiger Verlust des Bremsvermögens eines Hochgeschwindigkeitszuges, oder
- Nicht erkannte falsche Weichenlage auf einer Hauptstrecke“ (/16/).

Eine solche Beschreibung der Funktionsebene, auf die RAC-TS angewendet werden soll, erfolgte im Rahmen der Systemdefinition in Kapitel 4.2. Da RAC-TS in Anlehnung an das Sicherheitsziel für das europäische Zugsicherungssystem ETCS formuliert wurde, ist das zu betrachtende Gefährdungsszenario i_T im Rahmen der Kalibrierung für die Funktion ‚Zugbeeinflussung‘ definiert. Die zugehörige Funktion aus der Funktionsliste (siehe Anhang E: Funktionsliste) lautet:

| Ebene | | | Funktion (prEN) | Funktion (DIN) |
|-------|---|---|--|--|
| 1 | 2 | 3 | | |
| K | E | | Provide automatic train protection and control | Automatische Zugsicherung/-steuerung bereitstellen |

Laut der ETCS Functional Requirement Specification (FRS), Absatz 3.1.1.1 muss eine automatische Zugbeeinflussung sicherstellen, dass

- „die vorgegebenen Fahrgrenzen eingehalten werden, sowie
- die vorgeschriebene Geschwindigkeit eingehalten wird“ (aus dem Englischen /46/).

Diese werden im Folgenden als Subfunktionen der Funktion ‚Zugbeeinflussung‘ verstanden. Daraus lassen sich vereinfacht die folgenden Gefährdungsszenarien ableiten. Die Hauptgefährdung H für die Funktion lautet: ‚Zugbeeinflussung versagt unerkannt‘. Bei Betrachtung der Subfunktionen folgen daraus die Subgefährdungen:

- Vorgegebene Fahrgrenze wird nicht eingehalten, und/oder
- Vorgeschriebene Geschwindigkeit wird nicht eingehalten.

Als Folgen dieser Gefährdungen sind nachstehende Szenarien denkbar:

- Überschreitung der vorgegebenen Fahrgrenze (Fahrerlaubnis), und/oder
- Überschreitung der vorgeschriebenen Geschwindigkeit.

Im Folgenden wird das Gefährdungsszenario ‚Zugbeeinflussung versagt unerkannt‘ bewertet, um die Parameter G_T und S_T abzuleiten. Dazu werden die in Kapitel 6 vorgestellten BP-Risk-Tabellen angewendet.

7.2.2 Gefahrenabwehr G_T

Das Sicherheitsziel für ETCS-Fahrzeug- und Streckenausrüstung aus der TSI-CCS wurde aufgestellt für das Hochgeschwindigkeitsbahnsystem. Daher wird für das betriebliche Szenario eine Hochgeschwindigkeitsstrecke angenommen. Nach Tabelle 7-1 wird für Haupt- und Hochgeschwindigkeitsstrecken eine erhöhte Betriebsdichte angesetzt. Nach Angaben der DB AG Streckenstandards (/37/) fahren auf P160-300 Strecken bis zu 120 Zugpaare pro Tag. Dieses wird als Betriebsdichte eingestuft, die über dem Netzdurchschnitt liegt ($B_T = 3$).

Tabelle 7-1 Parameter Betriebsdichte

| B | Betriebsdichte | Beispiele |
|---|----------------|--|
| 1 | Gering | Unter Netzdurchschnitt, z. B. auf Güterverkehrsstrecken |
| 2 | Normal | Netzdurchschnitt, z. B. auf Regionalverkehrsstrecken |
| 3 | Erhöht | Über Netzdurchschnitt, z. B. auf Fern- oder HGV-Strecken |

Bei der Beurteilung der menschlichen Gefahrenabwehr wird zunächst festgestellt, dass der Triebfahrzeugführer (Tf) als externer Faktor bewertet werden kann, da er sich außerhalb der Zugbeeinflussungsfunktion des ETCS-Fahrzeuggeräts befindet. Er könnte zwar beim Versagen der Zugbeeinflussung möglicherweise noch eingreifen; RAC-TS gibt jedoch an, dass es keine oder nur wenige Barrieren gibt, die bei einem Funktionsversagen einen Unfall verhindern könnten. Außerdem gilt das Risikoakzeptanzkriterium RAC-TS für technische Systeme, bei denen der menschliche Einfluss vernachlässigbar ist (detaillierte Betrachtungen siehe Kapitel 7.3). Deswegen wird die menschliche Gefahrenabwehr anhand Tabelle 7-2 als fast nie möglich eingestuft ($M_T = 5$), da beim Hochgeschwindigkeitsverkehr nur noch ein zufälliges Eingreifen des Menschen die Gefahr abwenden könnte.

Tabelle 7-2 Parameter menschliche Gefahrenabwehr

| M | Menschliche Gefahrenabwehr | Beschreibung |
|---|----------------------------|---|
| 1 | Häufig möglich | Fertigkeits-basierende Handlung unter günstigen Umständen |
| 3 | Selten Möglich | Regel-basierende Handlung unter ungünstigen Umständen |
| 5 | Fast nie möglich | Zufälliges Eingreifen des Menschen |

Zusammenfassend ergeben die Werte der Subparameter B_T und M_T den Parameterwert für die Gefahrenabwehr $G_T = 3 + 5 = 8$.

7.2.3 Schadenspotenzial S_T

Wie vorhergehend beschrieben wird für das zu betrachtende Gefährdungsszenario i_T eine Hochgeschwindigkeitsstrecke angenommen. Laut /37/ kommen auf einer Hochgeschwindigkeitsstrecke ($v \geq 200$ km/h) vor allem Triebzüge zum Einsatz, deren maximale Last ca. 1000 t betragen. Dies entspricht beim Parameter Zuggattung laut Tabelle 7-3 dem Wert $T_T = 2$.

Tabelle 7-3 Parameter Zuggattung

| T | Zuggattung | Beispiele |
|---|------------|---|
| 1 | SPNV | Regionalbahn, Stadtexpress, S-Bahn Züge |
| 2 | SPFV + HGV | Triebzüge, bespannte Personenverkehrszüge, Nachtzüge, Autoreisezüge |
| 3 | SGV | Güterzüge (auch Schnellgüterzüge) |

Für HGV-Strecken wird nach Tabelle 7-4 die maßgebliche Geschwindigkeit als sehr hoch eingestuft, da die Leitgeschwindigkeiten laut DB AG Streckenstandards (/37/) bei über 230 km/h liegen. Der Parameter V_T hat also den Wert 4.

Tabelle 7-4 Parameter maßgebende Geschwindigkeit

| V | Maßgebende Geschwindigkeit | Beispiele |
|---|----------------------------|---|
| 1 | Gering | Rangieren, Fahrt auf Befehl oder Güterverkehrsstrecke |
| 2 | Mittel | Nebenstrecke |
| 3 | Hoch | Regionalverkehrsstrecke |
| 4 | Sehr Hoch | Fernverkehrsstrecke oder HGV-Strecke |

Bei einem unerkannten Versagen der Zugbeeinflussung sind mehrere Unfallszenarien denkbar. Für die zwei Subgefährdungsszenarien:

- Überschreitung der vorgegebenen Fahrgrenze (Fahrerlaubnis), und
- Überschreitung der vorgeschriebenen Geschwindigkeit,

können nach Tabelle 7-5 die folgenden Unfalltypen ausgewählt werden, nämlich

- Aufprall oder Zusammenstoß bei Verletzung der Fahrgrenzen,
- Entgleisung bei überhöhter Geschwindigkeit.

Ein Zusammenprall ist nicht möglich, da Bahnübergänge im HGV nicht erlaubt sind.

RAC-TS bezieht sich auf einen katastrophalen Schaden, bei dem es mehrere Tote und/oder Verletzte gibt. Somit wird der Unfalltyp ‚Aufprall‘ nicht betrachtet, da dabei in der Regel nur sehr geringe Personenschäden auftreten (siehe Tabelle 6-10). Zeitlich könnte vor einem Zusammenstoß bei Verletzung der Fahrgrenzen auch eine Entgleisung erfolgen, gerade bei sehr hohen Geschwindigkeiten. Um diese beiden Aspekte zu berücksichtigen, jedoch keine ‚worst-case‘-Betrachtung einzugehen, wird der Parameterwert A_T auf den Wert 4 gesetzt, der somit ‚zwischen‘ den beiden Szenarien ‚Entgleisung‘ und ‚Zusammenstoß‘ liegt.

Aus den Subparametern T_T , V_T , und A_T ergibt sich für das Schadenspotenzial S_T umfassend folgender Wert $S_T = 2 + 4 + 4 = 10$.

Tabelle 7-5 Parameter Unfalltyp

| A | Anzahl Betroffener | Beispiele (Unfalltypen) |
|---|---------------------|---|
| 1 | Einzelne Person | Bei einem Aufprall oder im Güterverkehr |
| 2 | Wenige Personen | Bei einem Zusammenprall |
| 3 | Einige Personen | Bei einer Entgleisung |
| 4 | Viele Personen | |
| 5 | Sehr viele Personen | Bei einem Zusammenstoß |

7.2.4 Zulässige Versagenshäufigkeit F

Nach der vereinfachten Folgen- und Konsequenzanalyse kann nun die BP-Risk-Tabelle für die zulässige Häufigkeit aufgestellt werden. Der Kalibrierungspunkt kann nach vorherigen geschätzten Werten errechnet werden zu: $G_T + S_T = 8 + 10 = 18$. Diesem Wert wird die tolerierbare Gefährdungsrate $f_T = 10^{-9}/h$ nach RAC-TS zugeordnet (siehe Tabelle 7-6).

Der Abstand der Häufigkeitswerte beträgt wie bei den anderen BP-Risk Tabellen $\sqrt{10}$. Die qualitative Beschreibung entspricht dem Häufigkeitswert in Jahren. Die THR kann allgemein auch mit Hilfe der Gleichung 7-3 berechnet werden:

$$THR = \sqrt{10}^{-(G+S)} \quad \text{Gleichung 7-3}$$

Anhand der Summe aus den Parametern G und S erhält somit der Anwender aus Tabelle 7-6 oder Gleichung 7-3 die zulässige Versagenshäufigkeit einer Systemfunktion. Die THR bezieht sich dabei auf ein System bestehend aus Mensch *und* Technik. Die Kalibrierung erfolgte jedoch an einem System ohne menschlichen Einfluss. Dieser Aspekt wird im folgenden Kapitel 7.3 noch einmal näher erläutert.

Tabelle 7-6 Skala zur Bestimmung der zulässigen Versagenshäufigkeit

| THR = $(\sqrt{10})^F$ (pro Funktion) | G + S | Beschreibung |
|--|--------------|----------------------------|
| $3 \cdot 10^{-5} /h$ | 9 | Einmal in 3 Jahren |
| $10^{-5} /h$ | 10 | Einmal in 10 Jahren |
| $3 \cdot 10^{-6} /h$ | 11 | Einmal in 30 Jahren |
| $10^{-6} /h$ | 12 | Einmal in 100 Jahren |
| $3 \cdot 10^{-7} /h$ | 13 | Einmal in 300 Jahren |
| $10^{-7} /h$ | 14 | Einmal in 1.000 Jahren |
| $3 \cdot 10^{-8} /h$ | 15 | Einmal in 3.000 Jahren |
| $10^{-8} /h$ | 16 | Einmal in 10.000 Jahren |
| $3 \cdot 10^{-9} /h$ | 17 | Einmal in 30.000 Jahren |
| $10^{-9} /h$ | 18 | Einmal in 100.000 Jahren |
| $3 \cdot 10^{-10} /h$ | 19 | Einmal in 300.000 Jahren |
| $10^{-10} /h$ | 20 | Einmal in 1.000.000 Jahren |

7.3 Exkurs: Mensch und Technik

Bei der Bahn gibt es eine Vielzahl von Systemen, die Sicherheitsverantwortung tragen. Diese Systeme sind zumeist sehr komplex und koppeln den Menschen und die Technik, um die geforderte Funktionalität und Verfügbarkeit zu erreichen. BP-Risk wird mit Hilfe des Risikoakzeptanzkriteriums RAC-TS kalibriert, was sich auf technische Systeme bezieht, in denen der Mensch keine sicherheitsrelevante Rolle spielt. Das Risikomodell von BP-Risk umfasst jedoch ein System von Mensch *und* Technik. Wie diese Kalibrierung für ein Mensch-Technik-System verstanden werden kann, wird im Folgenden dargelegt.

Es wird davon ausgegangen, dass es in einem System aus Mensch und Technik „*nur dann zu einem Schaden kommen kann, wenn vorher ein menschlicher Fehler oder ein technischer Ausfall vorgelegen hat; andererseits führt aber nicht jeder Fehler oder Ausfall auch zu einem Schaden, denn es ist möglich, dass der sicherheitsbeeinträchtigende Entwicklungsprozess vor dem Eintritt des Schadens gestoppt wird.*“ (/73/, Seite 81). Diese Aussage von Hinzen besagt, dass selbst nach einem menschlichen Fehler oder technischen Ausfall ein Schadenseintritt noch verhindert werden kann. Somit müssen sowohl Mensch als auch Technik versagen, damit es zum Schaden kommt. Deshalb wird in Abbildung 7-5 der vereinfachte Ereignis- und Fehlerbaum mit einer ‚UND‘-Verknüpfung dargestellt.

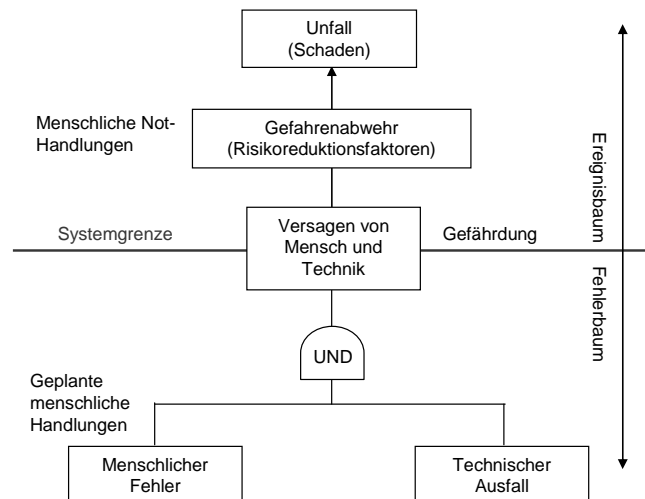


Abbildung 7-5 Versagen von Mensch und Technik (allgemein)

An der Systemgrenze eines Mensch-Maschine-Systems wird die Gefährdung ‚Versagen von Mensch und Technik‘ formuliert, die die Basis der Betrachtungen von BP-Risk darstellt. Diese Gefährdung kann durch einen Fehlerbaum zerlegt werden in zwei Ereignisse, nämlich nach obigem Zitat in ‚menschlicher Fehler‘ und ‚technischer Ausfall‘. Beide müssen auftreten, damit es zur Gefährdung kommt⁵⁰. Dies wird symbolisiert durch eine ‚UND‘ - Verknüpfung. In der Regel fällt zuerst die Technik aus und dann tritt ein menschlicher Fehler auf. In diesem Fall wird jedoch die Reihenfolge der Ausfälle nicht weiter betrachtet. Außerdem wird nur die Rückfallebene dargestellt, so dass gefährliche und hemmende Ausfälle nicht zusammen in einem Fehlerbaum abgebildet sind. D. h. die technischen Ausfälle, die ohne menschliches Einwirken sofort gefährlich sind, werden hier nicht dargestellt, könnten bei Bedarf aber über eine zusätzliche ‚ODER‘-Verknüpfung angefügt werden.

Zu beachten ist, dass innerhalb des Mensch-Maschine-Systems geplante (routinemäßige) menschliche Handlungen stattfinden. In Anlehnung an Hinzen handelt es sich hierbei um sogenannte ‚fertigungs-basierende Tätigkeiten‘ unter *normalen* Umständen. Tritt nun ein Fehler oder Ausfall auf, so muss auf der Rückfallebene agiert werden, bei dem es sich meist um ‚regel-basierte‘ Tätigkeiten handelt, d. h. der Mensch führt die Hilfsaktionen mit dem Wissen um die Regeln aus. ‚Wissens-basierte‘ Tätigkeiten, bei denen der Mensch sein Fachwissen nutzen muss, versucht man in der Praxis durch die Aufstellung von Regelwerken auszuschließen.

Bei der Kalibrierung von BP-Risk mit RAC-TS wird nun ein System betrachtet, bei dem davon ausgegangen wird, dass der Mensch keine oder geringe Sicherheitsverantwortung hat. Es wird angenommen, dass der menschliche Einfluss bei der Funktion ‚Zugbeeinflussung‘ im

⁵⁰ Anmerkung: Es wird oft diskutiert, ob menschliche Handlungen im Rahmen von Fehlerbäumen genauso behandelt werden dürfen wie technische Funktionen. Innerhalb der vorliegenden Arbeit wird diese Frage nicht detailliert betrachtet, sondern vorerst die pragmatische Herangehensweise aus der Praxis übernommen, da die Vereinfachung im Rahmen des Exkurses ausreichend genau ist.

ETCS-Level 2 vernachlässigbar ist. Daher befindet sich an der Systemgrenze als Gefährdung ausschließlich der technische Ausfall, der mit einer THR von $10^{-9}/h$ quantifiziert ist (siehe Abbildung 7-6).

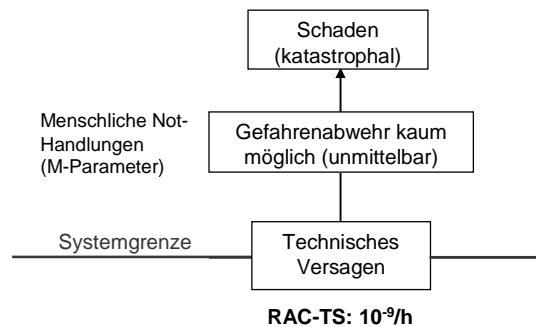


Abbildung 7-6 Kalibrierung mit RAC-TS

Daraus ergibt sich, dass der zuvor zum System gehörende Mensch (in diesem Fall der Triebfahrzeugführer) nun zur Systemumgebung gehört und somit als externer Faktor zur Gefahrenabwehr beitragen kann. RAC-TS gilt jedoch für Funktionsversagen, die ein unmittelbares Schadenspotenzial haben. Das bedeutet in diesem Fall, dass eine Gefahrenabwehr kaum möglich sein wird, da sich zwischen Unfall und Gefährdung keine signifikanten Barrieren befinden. Somit wird vorgegeben, dass der Mensch hier keine Eingriffsmöglichkeiten hat, was entsprechend beim Parameter *M* im Rahmen der Kalibrierung bewertet wurde (siehe 7.2.2).

Für die allgemeine Anwendung von BP-Risk wird weiterhin ein Mensch-Maschine-System betrachtet. Die zulässigen Häufigkeiten gelten für Mensch *und* Technik und müssen ggf. weiter aufgeteilt werden. Dies kann mit Hilfe von Fehlerbäumen durchgeführt werden. Bei der Risikobeurteilung wird dieser Part jedoch ausgeblendet, so dass quasi eine Black Box unterhalb der Systemgrenze angenommen wird, da noch nicht klar ist, inwieweit das System menschliche und/oder technische Komponenten enthält und vor allem in welchem Verhältnis sie zueinander stehen. Diese Betrachtungsweise wird illustriert in Abbildung 7-7.

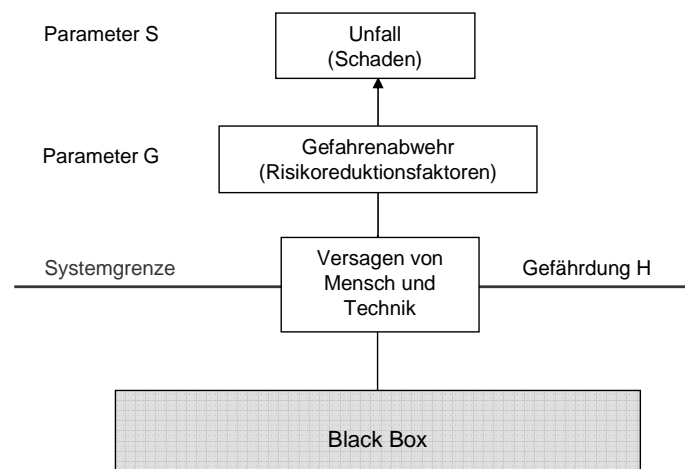


Abbildung 7-7 Versagen von Mensch und Technik (BP-Risk)

7.4 Zusammenfassung

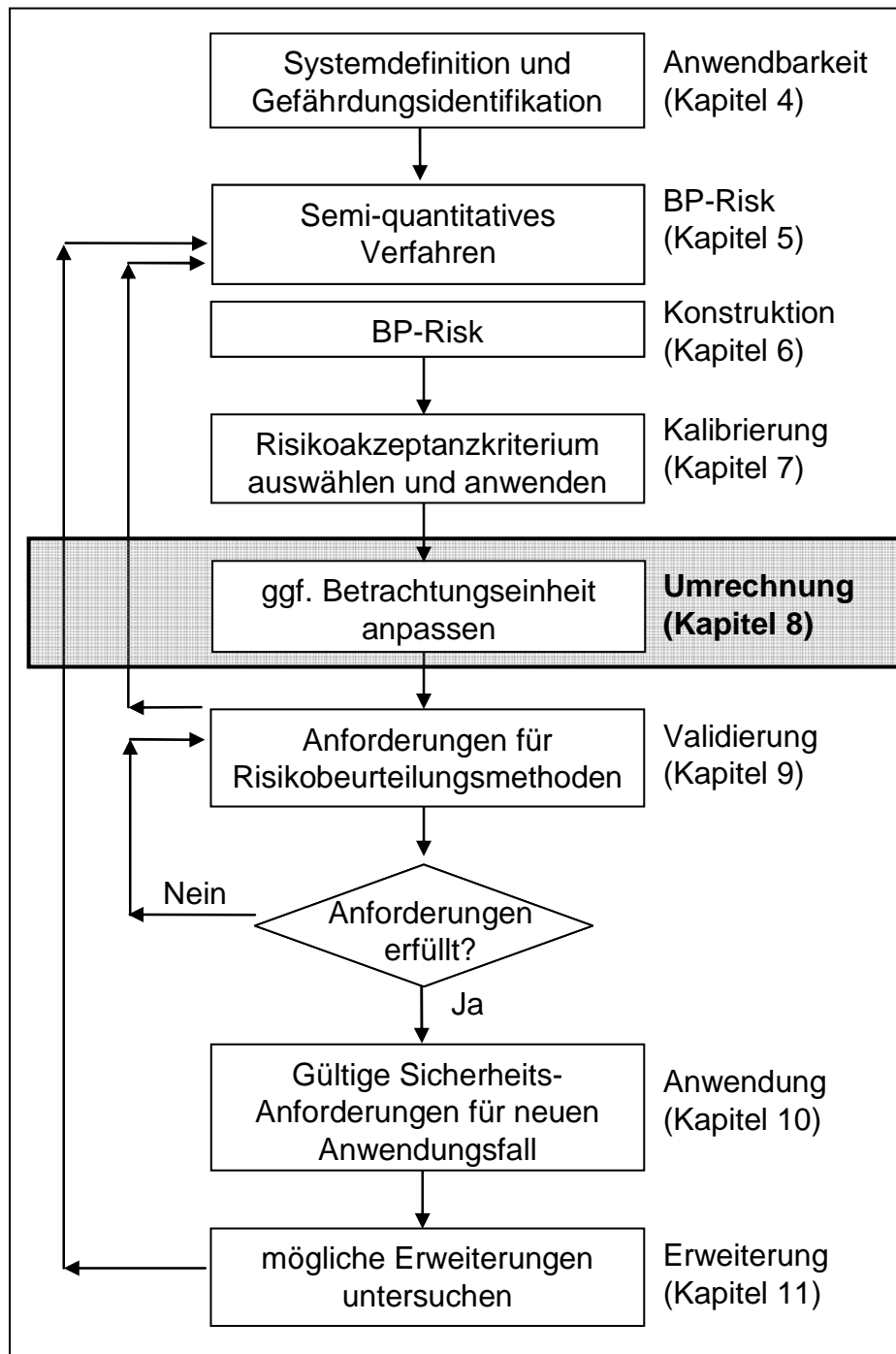
Die Kalibrierung von BP-Risk wurde anhand eines neuen europäischen Risikoakzeptanzkriteriums für technische Systeme (RAC-TS) erfolgreich durchgeführt und somit die Tabelle für die zulässige Versagengshäufigkeit aufgestellt.

Dazu wurde für ein gültiges (auf korrekter Ebene befindliches) Gefährdungsszenario die Kritikalität berechnet und anhand der tolerierbaren Gefährdungsrate von RAC-TS bewertet. Der tolerierbare Kritikalitätswert ist in der BP-Risk Häufigkeitstabelle implizit enthalten und kann nun mit Hilfe der BP-Risk Tabellen für beliebige Gefährdungsszenarien (auf korrekter Ebene!) angewendet werden.

Für BP-Risk ergeben sich damit Randbedingungen, die bei einer Anwendung unbedingt berücksichtigt werden müssen. Zum einen ist es äußerst wichtig, dass die korrekte Ebene betrachtet wird und zum anderen muss immer berücksichtigt werden, dass sich die Ergebnisse von BP-Risk auf ein Mensch-Technik-System beziehen.

Die durch die Kalibrierung festgelegte Systemebene von BP-Risk ist sicherlich nachteilig in Bezug auf die Flexibilität der Methode. Sie trägt jedoch positiv zur einfachen Anwendung und Vergleichbarkeit der Resultate bei. Die Automatisierung der Methodik könnte zusätzliche Verbesserungen der Anwendbarkeit bringen.

Im folgenden Kapitel 8 wird nun darauf eingegangen, wie die Ergebnisse von BP-Risk weiter verwendet werden können, was anhand von kurzen Beispielen erläutert wird.



8 Umrechnung

Laut dem Internationalen Technischen Komitee (ITC) der „Institution of Railway Signal Engineers“ (IRSE) hat sich gezeigt (/81/), dass Risikobeurteilungen, die in Übereinstimmung mit den Europäischen Normen und unter Berücksichtigung der spezifischen Details einer jeden Anwendung ausgeführt wurden, zu einer großen Kostensteigerung für Sicherheitsgenehmigungen geführt haben. Die Durchführung von separaten Risikobeurteilungen für jede einzelne Anlage in einem Land erhöht die Kosten ohne erkennbare Vorteile. Es besteht jedoch die Möglichkeit zu beträchtlichen Kostenreduzierungen bei Einführung generischer Analysen.

Anlagenunabhängige Risikobeurteilungen, wie sie von der ITC der IRSE gefordert werden, lassen dem Anwender Designfreiheit in der Umsetzung. Die Aufteilung einer THR auf die jeweiligen Subsysteme sollten nach eigenen Kriterien erfolgen können. Um dies zu gewährleisten, sollten die Risikobeurteilungen generisch sein, d. h. die Anzahl der Subsysteme und Komponenten sollten im Rahmen der Analyse keine Rolle spielen. Somit ist es sinnvoll, dass sich eine Risikobeurteilung nur auf die Systemfunktionen und ihre Gefährdungen bezieht und nicht weiter unterscheidet, wie diese Funktionen realisiert werden. Im Rahmen von BP-Risk erhält man deswegen als Ergebnis eine THR, die den Bezug ‚pro Funktion und pro Betriebsstunde‘ hat. Die Kalibrierung mit RAC-TS bestätigt diese generischen Herangehensweise, da *„der Ansatz von RAC-TS bedeutet, dass jede Versagensart auf der Systemebene getrennt betrachtet wird“* (/16/). Bei der zivilen Luftfahrt wurde diese Vereinfachung bereits erfolgreich eingeführt, was auch erheblich zur Kosteneffizienz beigetragen hat.

Im Gegensatz zur Luftfahrt werden in der Eisenbahntechnik jedoch viele Funktionen sowohl fahrzeug- als auch streckenseitig realisiert. Vergleichbare Streckenelemente, wie z.B. Weichen, Bahnübergänge oder auch Stellwerke der Eisenbahn gibt es in der Luftfahrt nicht. Daher ergibt sich dort auch nicht die Problematik, einen Wechsel der Bezugsgrößen vornehmen zu müssen. Die Ergebnisse einer Risikobeurteilung mit Hilfe von BP-Risk müssen jedoch weiter verwendbar sein, und zwar insbesondere für Streckenfunktionen. Im Folgenden wird daher an ausgewählten Beispielen gezeigt, wie mit Hilfe von Fehlerbäumen und Umrechnungsfaktoren die Versagenhäufigkeiten möglichst generisch aufgeteilt werden können.

8.1 Gefährdung an der Systemgrenze

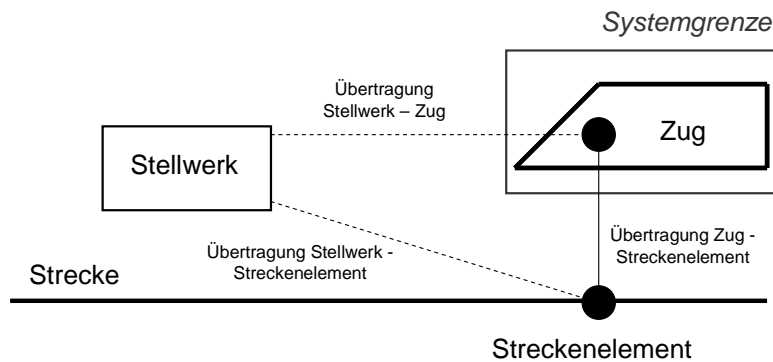


Abbildung 8-1 Systemdefinition BP-Risk

BP-Risk definiert als Betrachtungsgegenstand einen Zug (Systemgrenzen siehe Abbildung 4-4 und Abbildung 8-1). Es stellt sich nun die Frage, wie die Funktionen an den Schnittstellen, die sich nicht auf dem Zug befinden, bewerten lassen. Dazu ist unter anderem ein Wechsel der Bezugsgröße nötig. Die Anpassung der Bezugseinheit hängt allerdings von einer Vielzahl von Parametern ab, u. a. auch von der Betriebsdichte und der Art der Elemente, die die Funktion erbringen. Eine solche Umrechnung der Bezugsgröße kann mit Hilfe eines Fehlerbaums (FTA) erfolgen oder mit einem Umrechnungsfaktor. Ein generischer Fehlerbaum für eine solche Umrechnung ist in Abbildung 8-2 dargestellt.

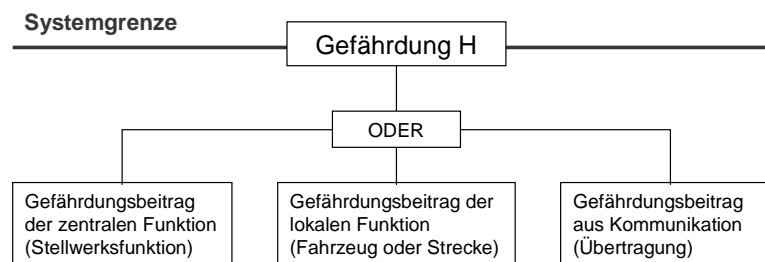


Abbildung 8-2 Generischer Fehlerbaum

Es wird davon ausgegangen, dass sich in der Regel die Gefährdung an der Systemgrenze aus drei Beiträgen zusammensetzt:

- Beitrag aus zentraler Funktion (z. B. wenn die Funktion von einem Stellwerk angesteuert wird),
- Beitrag aus lokaler Funktion (dabei ist zu unterscheiden, ob die Funktion z. B. auf dem Fahrzeug oder auf der Strecke realisiert ist), und
- Beitrag aus Kommunikation (z. B. Übertragung zwischen Strecke und Fahrzeug).

Der zentrale Gefährdungsbeitrag berücksichtigt einen möglichen falschen Befehl, der vom Stellwerk entweder an das Fahrzeug oder an ein Streckenelement gesendet wird. Der lokale Beitrag bezieht sich auf das Versagen des jeweiligen Elements an sich (fahrzeug- oder streckenseitig), auch wenn die Übertragung richtig funktioniert und das Stellwerk einen korrekten Befehl sendet.

Der Gefährdungsbeitrag aus der Kommunikation bezieht sich auf den Fall, dass zwar ein richtiger Befehl gesendet wird, er aber durch die Übertragung (oder Rückmeldung) verfälscht wird und somit ein falscher Befehl am Fahrzeug oder an der Strecke ankommt. Da die Kommunikation (Übertragung) in der Regel sehr sicher ausgeführt werden kann, wird im Folgenden vor allem auf die beiden Beiträge der lokalen und zentralen Funktionsanteile eingegangen.

8.2 Lokale Funktion

Nach (/85/) beträgt die Einheit für ein globales Risiko einer Personengruppe: „*Schadenseinheit pro Zeiteinheit*“. Für BP-Risk beträgt die Risikoeinheit konkret: ‚Opfer pro Stunde‘ pro Funktion. Die Gefahrenabwehr g ist einheitenlos, da dort Wahrscheinlichkeitswerte eingehen. Das Schadensausmaß wird in ‚Opfer‘ gemessen. Die Versagenshäufigkeit f hat die Einheit ‚Gefährdung (oder Funktionsversagen) pro Stunde‘.

Bei der Betrachtung des Gefährdungsbeitrags der lokalen Funktion wird nun unterschieden, ob die bewertete Funktion im Fahrzeug oder auf der Strecke realisiert wird. Wenn sich die Versagenshäufigkeit auf eine lokale Zugfunktion bezieht, erhält die THR folgende Einheit (siehe Gleichung 8-1).

$$f_{\text{Zug}} = \frac{\text{Gefährdung}}{\text{Zug} \cdot \text{Stunde}} = \frac{H}{\text{Zug} \cdot h} \quad \text{Gleichung 8-1}$$

Da der Betrachtungsgegenstand von BP-Risk ein Zug ist, gilt diese Einheit direkt für alle Funktionen der prEN 0015380. Dabei wird davon ausgegangen, dass ein Zug jeweils höchstens eine Funktion besitzt. Es gibt beispielsweise keine zwei Funktionen ‚Bremsen 1‘ und ‚Bremsen 2‘, sondern nur eine Funktion ‚Bremsen‘ (siehe Funktion GC in Funktionsliste). Diese Funktion kann dann möglicherweise durch mehrere Subsysteme (Subsystem 1 und Subsystem 2) realisiert werden.

Wenn es sich um eine lokale Streckenfunktion handelt, sollte sich die Einheit auf die Strecke und nicht auf den Zug beziehen. Für den Bezug auf die Strecke bietet sich die Einheit ‚Streckenkilometer‘ an (siehe Gleichung 8-2), da diese Einheit unabhängig ist von Betriebsprogrammen und technischen Komponenten.

$$f_{\text{Strecke}} = \frac{\text{Gefährdung}}{\text{Streckenkilometer} \cdot \text{Stunde}} = \frac{H}{\text{km} \cdot h} \quad \text{Gleichung 8-2}$$

Die fahrzeugseitige Versagenshäufigkeit f_{Zug} kann mit Hilfe eines Umrechnungsfaktor u auf die streckenseitige Versagenshäufigkeit f_{Strecke} umgerechnet werden. Dabei wird eine multiplikative Beziehung angenommen (siehe Gleichung 8-3).

$$f_{\text{Strecke}} = f_{\text{Zug}} \cdot u \quad \text{Gleichung 8-3}$$

Der Umrechnungsfaktor u (siehe Gleichung 8-4) kann berechnet werden aus der Streckenbelastung (Einheit: ‚Zug pro Stunde‘) und der mittleren Reisegeschwindigkeit (Einheit: ‚Streckenkilometer pro Stunde‘). Konkret besagt der Umrechnungsfaktor, wie viele Züge sich auf einem Streckenkilometer befinden, was betrieblich der Zugdichte⁵¹ entspricht.

$$u = \frac{\left(\frac{\text{Zug}}{h}\right)}{\left(\frac{\text{km}}{h}\right)} = \frac{\text{Zug}}{\text{km}} \quad \text{Gleichung 8-4}$$

Die mittlere Reisegeschwindigkeit berücksichtigt dabei, dass ein Zug auf seiner Fahrt nicht immer mit der Streckenhöchstgeschwindigkeit fährt, sondern durch die Halte in den Bahnhöfen Beschleunigungs- und Bremsphasen hat und zusätzlich auch Aufenthaltszeiten in den Bahnhöfen anfallen. Deswegen kann die mittlere Reisegeschwindigkeit für einige Zuggattungen und Streckenkategorien weniger als 50% der Streckenhöchstgeschwindigkeit betragen. Tabelle 8-1 gibt einige Beispiele für durchschnittliche Reisegeschwindigkeiten in Abhängigkeit der Zuggattungen.

Tabelle 8-1 Durchschnittliche Reisegeschwindigkeiten (nach /1/, /6/, /3/)

| Zuggattung | Beispiel | Höchstgeschwindigkeit | Durchschnittl. Reisegeschw. |
|---------------------------|-------------------------|-----------------------|-----------------------------|
| HGV | ICE | 200 km/h und mehr | 135 km/h |
| Schneller SPFV | IC/EC | bis zu 200 km/h | 108 km/h |
| SPFV mit regionalem Bezug | IR, D-Tag ⁵² | bis zu 160 km/h | 93 km/h ⁵³ |
| Schneller SPNV | RE | bis zu 120 km/h | 90 km/h |
| SPNV | RB, N ⁵⁴ | bis zu 80 km/h | 60 km/h |
| SGV | | bis zu 50 km/h | 18 km/h |

Detaillierte Betrachtungen für die unterschiedlichen Geschwindigkeiten und Zugdichten im Bahnhof und auf der Strecke müssten separat ausgerechnet werden, um sie für den Umrechnungsfaktor zu berücksichtigen. Zur Vereinfachung wird für den Umrechnungsfaktor mit der mittleren Reisegeschwindigkeit V_R und der mittleren Zugdichte gerechnet.

Die mittlere Streckenauslastung⁵⁵ wird ermittelt aus den Tagesganglinien der Streckenstandards der DB-AG (/37/). Dabei wird immer die Obergrenze der Streckenauslastung betrachtet, da laut DB-Richtlinie dies der Zielgröße entspricht. Die Verstärkung von SGV, SPNV in den Tagesganglinien werden vorerst nicht berücksichtigt. Bei Mischbetrieb wurde der jeweilige Mittelwert für SGV, SPNV und SPFV berechnet.

⁵¹ Anzahl der Züge je Längeneinheit angegebene räumliche Dichte der Züge auf einer Strecke (/95/).

⁵² D-Zug (Schnellzug): alte Zuggattung der DB-AG.

⁵³ Mittelwert für IR (97 km/h) und D-Tag (88 km/h).

⁵⁴ Nahverkehrszug: alte Zuggattung der DB-AG (Vorläufer der Regionalbahn).

⁵⁵ Der Durchsatz einer Strecke in Zügen/Zeiteinheit wird als Belastung bezeichnet. Die in der 413 genannte Streckenauslastung meint diejenige Belastung, bei der die Strecke als ausgelastet gilt, auf die also die Dimensionierung der Strecke auszurichten ist.

Mit Hilfe der mittleren Reisegeschwindigkeit V_R und der mittleren Auslastung kann der Umrechnungsfaktor für die jeweilige Streckenkategorie bestimmt werden. Die resultierenden Werte für u in Tabelle 8-2 liegen zwischen $2 \cdot 10^{-2}$ und $4 \cdot 10^{-2}$. Das entspricht in der BP-Risk Häufigkeitstabelle ca. drei Stufen, weil die Basis Wurzel 10 zugrunde liegt. Nach /16/ sind „die Sicherheitsleistungen einer Einrichtung an der Strecke [...] meist bedeutend höher [...]“, was durch diese Einheitenumrechnung bestätigt wird.

Tabelle 8-2 Umrechnungsfaktor

| Standard | V_R [km/h] | Auslastung [Zug/h] | u [Zug/km] |
|----------|-----------------|-----------------------|-----------------|
| HGV | 135 | 5,00 | 0,037 |
| SPFV230 | 108 | 3,86 | 0,036 |
| SPFV160 | 93 | 3,05 | 0,033 |
| SPNV120 | 90 | 2,06 | 0,023 |
| SPNV80 | 60 | 1,33 | 0,022 |
| SGV | 18 | 0,42 | 0,023 |

Diese Umrechnung könnte im Rahmen von BP-Risk pauschal dadurch berücksichtigt werden, dass die Häufigkeitstabelle mit dem Wert S+G+3 ausgewertet wird, wenn es sich um eine Streckenfunktion handelt. Der Vorteil wäre, dass man immer noch eine generische Betrachtung hätte. Nachteilig wäre, dass man dann wieder Annahmen für die Aufteilung der Häufigkeit im Rahmen des Fehlerbaums aus Abbildung 8-2 treffen müsste, also beispielsweise, dass die lokale Funktion immer die Hälfte des Gefährdungsbeitrages bekommt, was wiederum erneut durch einen konstanten Faktor berücksichtigt werden müsste. Im Folgenden wird diese Pauschalisierung nicht vorgenommen, es bleibt jedoch zu prüfen, ob beispielsweise eine Einteilung in Klassen eine generische Umrechnung möglich macht.

In früheren Ansätzen von BP-Risk und auch bei anderen Methoden zur Risikobeurteilung, spielt die Gefährdungsdauer eine Rolle. Im Rahmen der Konstruktion (siehe Kapitel 5.3.1) wurde bereits herausgearbeitet, dass die Gefährdungsdauer im Rahmen von BP-Risk betrieblich nur für streckenseitige Funktionen relevant ist. Es wird davon ausgegangen, dass vor allem die Offenbarung durch einen anderen Zug zur Gefahrenabwehr beiträgt, da die Zeit zwischen den Wartungsintervallen in der Regel sehr viel länger ist, als die Zeit zwischen zwei Zügen. Somit hängt die Wahrscheinlichkeit, dass ein Zug aufgrund eines streckenseitigen Funktionsversagens auf eine Gefährdung trifft, vor allem von der Zugdichte, aber auch von den gefahrenen Geschwindigkeiten und der Häufigkeit der Einwirkung durch ein Streckenelement ab⁵⁶ (siehe Abbildung 8-3).

⁵⁶ Dieses Risikomodell gilt nicht für solche Streckenelemente, die ‚funktional‘ miteinander verbunden sind, wie z. B. Balisen oder Heißläuferortungsanlagen. Für solche Komponenten existiert das Paradoxon, dass je mehr Elemente im Gleis liegen, desto wahrscheinlicher ist es, dass ein Zug auf eine ausgefallene Komponente trifft aber auch desto eher kann ein Ausfall detektiert werden (z. B. bei verlinkten Balisen). Es ist jedoch denkbar, dass sich diese Effekte ausgleichen.

Die Gefährdungsdauer wird dabei implizit durch den Umrechnungsfaktor u berücksichtigt, der sich aus der Auslastung und der mittleren Reisegeschwindigkeit zusammensetzt.

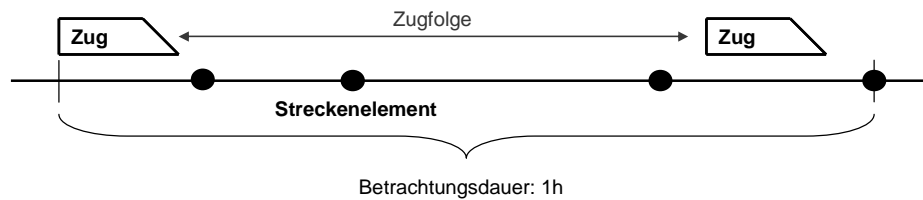


Abbildung 8-3 Risikomodell für Streckenfunktionen

Da der Anwender als Ergebnis nicht eine Versagenshäufigkeit pro Streckenkilometer, sondern idealerweise pro Streckenelement erhalten möchte, ist es notwendig, die Anzahl der Streckenelemente in einem zweiten Umrechnungsschritt mit zu berücksichtigen. Insgesamt ergibt sich formal folgende Umrechnung (siehe Gleichung 8-4).

$$\frac{\text{Zug}}{\text{Streckenelement}} = u \cdot \frac{\text{km}}{\text{Streckenelement}} \quad \text{Gleichung 8-5}$$

8.3 Beispiele

Im Folgenden soll für Streckenelemente gezeigt werden, wie die Ergebnisse der umgerechneten Bezugsgröße weiterverwendet werden können. Dabei werden beispielhaft Bahnübergänge und Weichen betrachtet, da für diese Streckenelemente ausreichend Daten zur Verfügung standen. Diese Aufteilung ist jedoch auch für alle anderen Streckenelemente wie Signale, Gleismagnete, Achszähler, Balisen (siehe Fußnote 56), usw. möglich.

8.3.1 Bahnübergänge

Für die Berechnung einer Versagenshäufigkeit für ein Streckenelement wird im Folgenden ein Bahnübergang (BÜ) bewertet (siehe Abbildung 8-4).

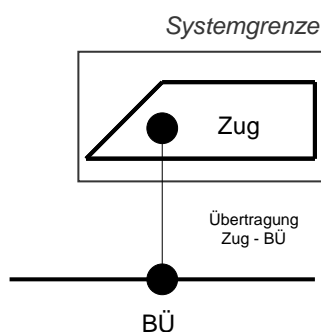


Abbildung 8-4 Schnittstelle Zug - BÜ

Die zugehörige Funktion aus der Funktionsliste befindet sich an der Schnittstelle zur Funktion KGC und lautet: „BÜ sichern“ (siehe Tabelle 8-3).

Tabelle 8-3 Funktion LH aus Funktionsliste

| Ebene | | | Funktion | Erläuterung |
|-------|---|---|--------------------------------|-----------------------------------|
| 1 | 2 | 3 | | |
| K | G | C | Signale steuern und überwachen | Funktionsgruppe aus prEN0015380-4 |
| L | B | H | BÜ sichern | Zusätzliche Streckenfunktion |

Aus Sicht des Fahrzeugs bedeutet diese Funktion der Schutz des Bahnverkehrs vor kreuzenden Kraftfahrzeugen (Straßenverkehrsteilnehmern). Die daraus abgeleitete vereinfachte Gefährdung lautet: ‚BÜ nicht gesichert‘. Damit ist gemeint, dass die BÜSA sowohl für den Bahnbetrieb als auch für den Straßenverkehr unerkannt versagt. In Kapitel 4.3.1 wurde bereits eine funktionale FMEA für das Beispiel BÜ durchgeführt. Danach sind detaillierte Ausfallmodi, wie die vorzeitige Ein- und Ausschaltung im Falle einer zugüberwachten BÜ-Anlage möglich. Das System einer zugüberwachten (Überwachung ÜS) Anlage wird nun auch im folgenden Beispiel betrachtet.

Technisch gesicherte Bahnübergänge kommen in allen Betriebsarten und Geschwindigkeiten bis 160 km/h vor. Zur Bewertung mit BP-Risk wird eine Nahverkehrsstrecke angenommen, für die nach Tabelle 8-4 eine normale Betriebsdichte angesetzt wird ($B = 2$).

Tabelle 8-4 Parameter Betriebsdichte

| B | Betriebsdichte | Beispiele |
|---|----------------|--|
| 1 | Gering | Unter Netzdurchschnitt, z. B. auf Güterverkehrsstrecken |
| 2 | Normal | Netzdurchschnitt, z. B. auf Regionalverkehrsstrecken |
| 3 | Erhöht | Über Netzdurchschnitt, z. B. auf Fern- oder HGV-Strecken |

Zur menschlichen Gefahrenabwehr können sowohl der Triebfahrzeugführer (Tf) als auch die Straßenverkehrsteilnehmer beitragen. Da in den meisten Fällen nicht davon ausgegangen werden kann, dass der Tf bei Versagen der BÜ-Sicherung die Geschwindigkeit noch erheblich reduzieren kann, wird in diesem Fall die menschliche Gefahrenabwehr durch den Tf als fast nie möglich eingestuft. Eine menschliche Gefahrenabwehr ist jedoch möglich durch eine Notreaktion des Straßenverkehrsteilnehmers, allerdings stark abhängig von örtlichen Gegebenheiten (Bebauung, Wetter, Tageszeit, Verkehrsdichte, usw.), so dass von einer stärkeren Risikoreduktion nicht ausgegangen wird. Die Gefahrenabwehr wird anhand von Tabelle 8-5 als möglich eingestuft ($M = 3$), da bei zwei menschlichen Handlungen die Erfolgversprechendste bewertet werden soll (siehe Kapitel 6.1.2).

Tabelle 8-5 Parameter menschliche Gefahrenabwehr

| M | Menschliche Gefahrenabwehr | Beschreibung |
|---|----------------------------|---|
| 1 | Häufig möglich | Fertigkeits-basierende Handlung unter ungünstigen Umständen |
| 3 | Selten möglich | Regel-basierende Handlungen unter ungünstigen Umständen |
| 5 | Fast nie möglich | Zufälliges Eingreifen des Menschen |

Zusammenfassend ergeben die Werte der Subparameter B und M den Parameterwert für die Gefahrenabwehr $G = 2 + 3 = 5$.

Tabelle 8-6 Parameter Zuggattung

| T | Zuggattung | Beispiele |
|---|------------|---|
| 1 | SPNV | Regionalbahn, Stadtexpress, S-Bahn Züge |
| 2 | SPFV + HGV | Triebzüge, bespannte Personenverkehrszüge, Nachtzüge, Autoreisezüge |
| 3 | SGV | Güterzüge (auch Schnellgüterzüge) |

Wie vorhergehend beschrieben, wird für das zu betrachtende Gefährdungsszenario eine Nahverkehrsstrecke angenommen. Laut Tabelle 8-6 wird der Wert für die Zuggattung im spurgeführten Nahverkehr (SPNV) mit $T = 1$ bewertet. Für Nahverkehrsstrecken wird nach Tabelle 8-7 die maßgebliche Geschwindigkeit als hoch eingestuft. Der Parameter V erhält also den Wert 3.

Tabelle 8-7 Parameter maßgebende Geschwindigkeit

| V | Maßgebende Geschwindigkeit | Beispiele |
|---|----------------------------|---|
| 1 | Gering | Rangieren, Fahrt auf Befehl oder Güterverkehrsstrecke |
| 2 | Mittel | |
| 3 | Hoch | Nebenstrecke oder Regionalverkehrsstrecke |
| 4 | Sehr Hoch | Fernverkehrsstrecke oder HGV-Strecke |

Bei Unfällen an Bahnübergängen kommen in der Regel die beteiligten Straßenverkehrsteilnehmer sowie ggf. der Tf ernsthaft zu Schaden. Unfälle mit vielen Opfern bilden die Ausnahme. Der Wert für Parameter A wird anhand von Tabelle 8-8 zu $A = 2$ bestimmt, da die typische Unfallfolge an einem BÜ ein ‚Zusammenprall‘ ist.

Tabelle 8-8 Parameter betroffene Personen

| A | Anzahl Betroffener | Beispiele (Unfalltyp) |
|---|---------------------|---|
| 1 | Einzelne Person | Bei einem Aufprall oder im Güterverkehr |
| 2 | Wenige Personen | Bei einem Zusammenprall |
| 3 | Einige Personen | Bei einer Entgleisung |
| 4 | Viele Personen | |
| 5 | Sehr viele Personen | Bei einem Zusammenstoß |

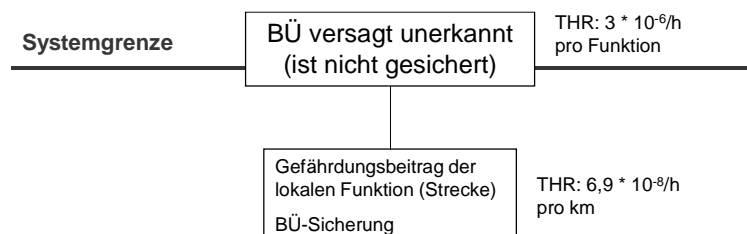
Aus den Subparametern T , V , und A ergibt sich für das Schadenspotenzial S zusammenfassend folgender Wert $S = 1 + 3 + 2 = 6$. Anhand der Summe aus den Parametern G und S ($G + S = 11$) wird mit Hilfe der Tabelle 8-9 die zulässige Versagenshäufigkeit bestimmt zu $3 \cdot 10^{-6}/h$ pro Funktion, also einem tolerierbaren gefährlichen Versagen in 30 Jahren.

Tabelle 8-9 Skala zur Bestimmung der zulässigen Versagshäufigkeit

| THR | G + S | Beschreibung |
|----------------------|-------|----------------------|
| 10^{-4} /h | 8 | Einmal jährlich |
| $3 \cdot 10^{-5}$ /h | 9 | Einmal in 3 Jahren |
| 10^{-5} /h | 10 | Einmal in 10 Jahren |
| $3 \cdot 10^{-6}$ /h | 11 | Einmal in 30 Jahren |
| 10^{-6} /h | 12 | Einmal in 100 Jahren |
| $3 \cdot 10^{-7}$ /h | 13 | Einmal in 300 Jahren |

Der für den Fall BÜ konkretisierte Fehlerbaum ist in Abbildung 8-5 dargestellt. Damit kann die Versagshäufigkeit von BP-Risk weiter aufgeteilt werden. Da wie oben erwähnt, die ÜS-Anlagen keine Verbindung zum Stellwerk haben, entfällt der Gefährdungsbeitrag der zentralen Funktion. Auch der Beitrag aus der Kommunikation entfällt hier, da eine Übertragung zwischen Fahrzeug und der Ein- und Ausschaltung nicht stattfindet. Die Radsensoren detektieren das vorbeifahrende Fahrzeug – es werden jedoch keine Informationen im eigentlichen Sinne übertragen.

Die THR der lokalen Funktion beträgt somit $3 \cdot 10^{-6}$ /h. Das Fahrzeug hat keinen Anteil an dieser Funktion, so dass die THR für den Bezug auf die Strecke mit Hilfe des Umrechnungsfaktors u aus Tabelle 8-2 umgerechnet wird. Dabei wird für den Nahverkehr eine SPNV 120 angenommen. Somit beträgt die THR für die Strecke $3 \cdot 10^{-6}$ /h $\cdot 0,023 \approx 6,9 \cdot 10^{-8}$ /h pro Streckenkilometer.

**Abbildung 8-5 Fehlerbaum BÜ**

Um die THR pro Streckenelement zu erhalten ist eine weitere Umrechnung nötig, die die Anzahl der Streckenelemente pro Kilometer berücksichtigt. Laut DB-Jahresbericht /36/ befinden sich insgesamt 20.317 Bahnübergänge im Netz der DB AG, was eine Betriebslänge von 34.128,4 km hat. Da Bahnübergänge im Fern- und Hochgeschwindigkeitsverkehr nicht vorkommen, wird die Anzahl der Bahnübergänge auf die Strecken des SPFV 160, SPNV und SGV aufgeteilt. Die prozentuale Einteilung der Betriebskilometer erfolgt nach den Vorgaben der Netz 21 Strategie der DB AG. Die detaillierte Berechnung befindet sich im Anhang dieser Arbeit (siehe Anhang F: Berechnung BÜ). Nach Expertenschätzung wird für die Strecken des SPFV 160 und SPNV 120 angenommen, dass sich ca. alle 3km ein BÜ befindet. Für die Strecken des SPNV 80 und SGV wird angenommen, dass sich ca. alle 1km ein BÜ befindet.

Der Kehrwert (km pro BÜ) kann verstanden werden als die Anzahl der Kilometer, die sich durchschnittlich zwischen zwei Bahnübergängen auf der Strecke befinden. Mit diesem Wert wird die neue THR bestimmt. Sie beträgt für eine SPNV 120-Strecke:

$$6,9 \cdot 10^{-8} / \text{h pro km} \cdot 3,0 \text{ km pro BÜ} = 2,07 \cdot 10^{-7} / \text{h pro BÜ}.$$

Es ist wichtig zu erwähnen, dass diese Anforderung für ein System gilt, das aus Mensch und Technik besteht. Wenn man den untersuchten Bahnübergang jedoch weitestgehend durch Technik sichert, so liegt das vorliegende Ergebnis in derselben Größenordnung wie die Sicherheitsanforderung für Bahnübergänge, die beispielhaft anhand der Risikoformel ermittelt wurde (siehe /9/, Seite 47).

8.3.2 Weiche

Für die Berechnung einer Versagenshäufigkeit mit lokalem und zentralem Funktionsanteil wird im Folgenden beispielhaft eine Weiche bewertet. Dabei wird davon ausgegangen, dass die Weiche vom Stellwerk angesteuert wird (siehe Abbildung 8-6).

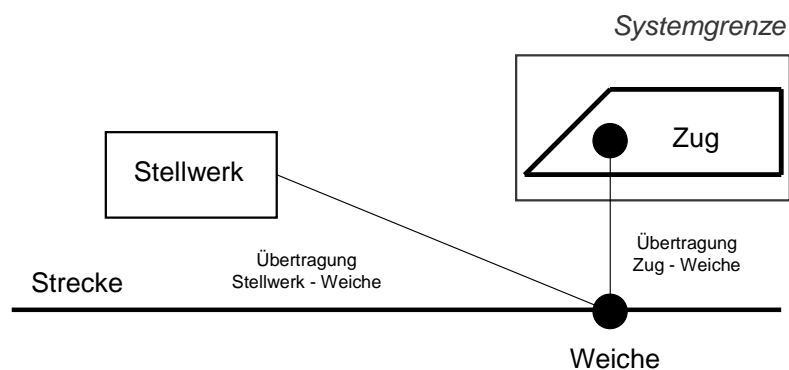


Abbildung 8-6 Systemdefinition Weiche

Die zugehörige Funktion aus der Funktionsliste befindet sich an der Schnittstelle zur Funktion KGB und lautet: „*Bewegliche Fahrwegelemente sichern*“ (siehe Tabelle 8-10).

Tabelle 8-10 Funktion LG

| Ebene | | | Funktion | Erläuterung |
|-------|---|---|---------------------------------|-----------------------------------|
| 1 | 2 | 3 | | |
| K | G | B | Streckenführung wählen | Funktionsgruppe aus prEN0015380-4 |
| L | B | G | Bewegl. Fahrwegelemente sichern | Zusätzliche Streckenfunktion |

Die daraus abgeleitete vereinfachte Gefährdung würde lauten: ‚bewegliches Fahrwegelement nicht gesichert‘. Für eine Weiche wären verschiedene Ausfallmodi denkbar (/66/, Seite 193), z. B. ‚Weiche läuft zur Unzeit um‘ (Weichenstellung unter einem Fahrezug) oder ‚Weiche liegt unerkannt in falscher Lage‘ (falsche Weichenstellung).

Zur Bewertung mit BP-Risk wird für dieses Beispiel eine Hochgeschwindigkeitsstrecke angenommen. Nach Tabelle 8-4 wird für Haupt- und Hochgeschwindigkeitsstrecken eine erhöhte Betriebsdichte angesetzt ($B = 3$). Bei der Beurteilung der menschlichen Gefahrenabwehr wird zunächst festgestellt, dass der Tf als externer Faktor bewertet werden kann, da er selbst die Fahrwegsicherung nicht vornimmt. Allerdings wird es als unwahrscheinlich angenommen, dass der Tf im Hochgeschwindigkeitsverkehr eine falsch liegende oder umlaufende Weiche bemerkt und dann noch rechtzeitig eingreifen kann. Deswegen wird die menschliche Gefahrenabwehr anhand Tabelle 8-5 als fast nie möglich eingestuft ($M = 5$).

Zusammenfassend ergeben die Werte der Subparameter B und M den Parameterwert für die Gefahrenabwehr $G = 3 + 5 = 8$.

Wie vorhergehend beschrieben, wird für das zu betrachtende Gefährdungsszenario eine Hochgeschwindigkeitsstrecke angenommen. Laut [37] kommen auf einer Hochgeschwindigkeitsstrecke ($v \geq 200$ km/h) vor allem Triebzüge zum Einsatz, was beim Parameter Zuggattung laut Tabelle 8-6 dem Wert $T = 2$ entspricht. Für HGV-Strecken wird nach Tabelle 8-7 die maßgebliche Geschwindigkeit als sehr hoch eingestuft ($V = 4$). Bei einem unerkannten Versagen der Fahrwegsicherung wird nach Tabelle 8-8 die Entgleisung als typische Unfallfolge angenommen, was dem Wert $A = 3$ entspricht.

Aus den Subparametern T , V , und A ergibt sich für das Schadenspotenzial S zusammenfassend folgender Wert $S = 2 + 4 + 3 = 9$. Anhand der Summe aus den Parametern G und S ($G + S = 17$) wird mit Hilfe der Tabelle 8-9 die zulässige Versagenshäufigkeit bestimmt zu $3 \cdot 10^{-9}$ /h pro Funktion.

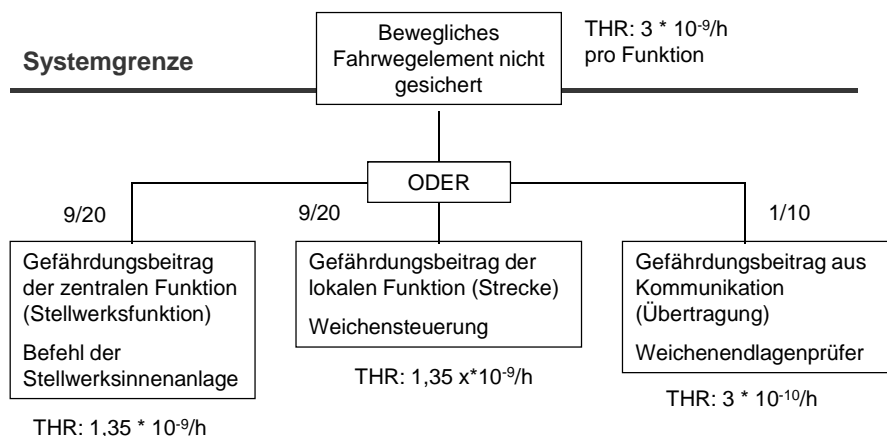


Abbildung 8-7 Fehlerbaum Weiche

Anhand des Fehlerbaums in Abbildung 8-7 kann diese Versagenshäufigkeit von BP-Risk weiter aufgeteilt werden. Da, wie oben erwähnt, die Kommunikation sehr sicher ausgeführt werden kann, wird dem Gefährdungsbeitrag aus der Übertragung vereinfacht $1/10$ zugeschrieben. Die Beiträge aus zentraler und lokaler Funktion erhalten jeweils $9/20$. Diese Aufteilungen sind Entscheidungen, die zur Designfreiheit gehören und die im konkreten Fall nach eigenen Kriterien erfolgen können.

Die THR der lokalen Funktion beträgt somit $3 \cdot 10^{-9}/h \cdot 0,45 = 1,35 \cdot 10^{-9}/h$. Das Fahrzeug hat keinen Anteil an dieser Funktion, so dass die THR für den Bezug auf die Strecke mit Hilfe des Umrechnungsfaktors für eine HGV-Strecke aus Tabelle 8-2 umgerechnet wird. Somit beträgt die THR für die Strecke $1,35 \cdot 10^{-9}/h \cdot 0,037 \approx 5 \cdot 10^{-11}/h$ pro Streckenkilometer.

Zur weiteren Umrechnung für den Bezug pro Streckenelement werden Daten aus den DB-Streckenstandards (/37/) herangezogen. Laut Streckenstandards befinden sich ca. vier Überleitstellen auf einer 100km langen HGV-Strecke (siehe Abbildung 8-8).

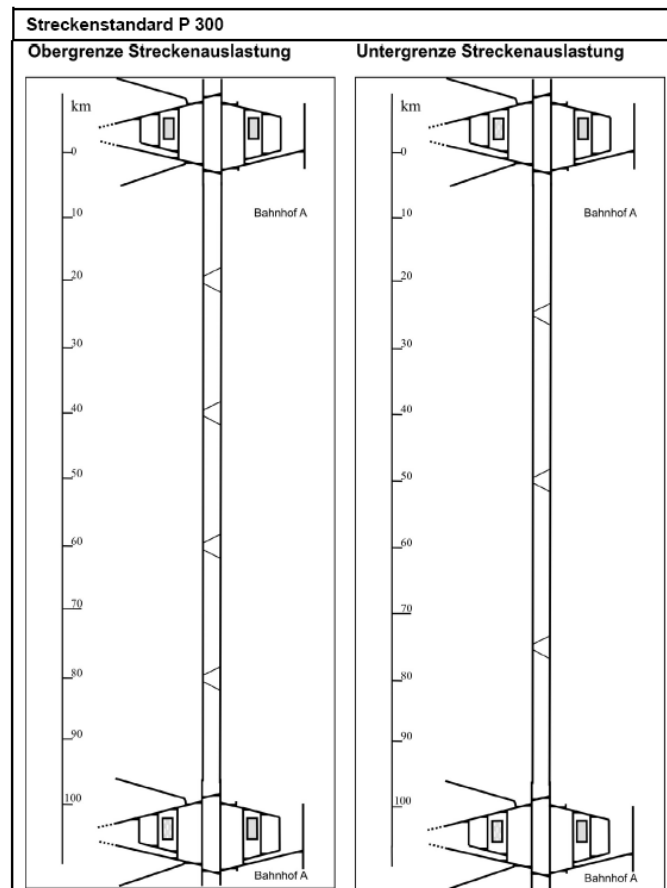


Abbildung 8-8 Streckenstandard HGV (/37/)

Jede Überleitstelle hat vier Weichen, die befahren werden können, so dass auf freier Strecke ein Zug ca. 8 Weichen auf 100 km begegnen kann. Die Streckenstandards sehen auf den 100 km langen Streckenabschnitt im HGV keine Bahnhöfe vor, so dass die Weichen in den Bahnhöfen unberücksichtigt bleiben. Diese werden auch mit geringeren Geschwindigkeiten befahren, so dass dies einem anderen Gefährdungsszenario entsprechen würde. Um nun die THR pro Weiche auszurechnen, wird die Versagenshäufigkeit mit der Anzahl der km multipliziert, die sich im Mittel zwischen zwei Weichen befindet, also $100 \text{ km} / 8 \text{ Weichen} = 12,5 \text{ km pro Weiche}$. Dabei wird vernachlässigt, dass die Weichen in den Überleitstellen zum Teil sehr nahe beieinander liegen.

Die THR pro Weiche errechnet sich dann zu: $5 \cdot 10^{-11}/h \cdot 12,5 = 6,25 \cdot 10^{-10}/h$ pro Weiche. Dies entspricht einer tolerierbaren Gefährdung pro Weiche in ca. 150.000 Jahren.

8.3.3 Zentrale Funktion

Die THR der zentralen Funktion im Fehlerbaum aus Abbildung 8-7 hat die Einheit Gefährdung pro Stunde und pro Funktion. Diese Anforderung kann nun direkt an die Schnittstelle der Innenanlage eines Stellwerks gestellt werden und würde somit für eine Stellwerksfunktion gelten. Im obigen Beispiel für die Weiche wäre die Gefährdung der Stellwerksfunktionalität beispielsweise die ‚Ausgabe des falschen Stellkommandos an die Weiche‘. Der Wert für dieses Funktionsversagen wäre aus obigem Beispiel: $THR = 1,35 \cdot 10^{-9}/h$, was in derselben Größenordnung wie die Sicherheitsanforderung für die Schnittstelle Weiche eines elektronischen Stellwerkes liegt.

Es stellt sich nun die Frage, inwiefern zu berücksichtigen ist, wie viele Elemente ein solches Stellwerk ansteuert. Es kann angenommen werden, dass sich ein Fehler der Stellwerksinnenanlage nicht sofort auf alle angesteuerten Elemente auswirkt. Je mehr Elemente im Stellbereich liegen, desto geringer wäre demnach die Wahrscheinlichkeit, dass das betrachtete Element von einem Funktionsversagen des Stellwerks betroffen ist. Somit würde die Sicherheitsanforderung immer weniger streng werden, je mehr Elemente angesteuert werden. Die THR könnte umgerechnet werden, indem sie mit der Anzahl der angesteuerten Elemente multipliziert wird (siehe Gleichung 8-6).

$$f_{Stellwerk} = f \cdot \frac{Elemente}{Funktion} = \frac{H \cdot Element}{h \cdot Funktion} \quad \text{Gleichung 8-6}$$

Als Betrachtungsnormale könnte die Anzahl der Stelleinheiten pro Stellwerkstyp dienen, die beispielsweise von /5/ berechnet wurden (siehe Tabelle 8-11). Dabei beinhaltet eine Stelleinheit „*exakt die fachlichen Komponenten*“

- Weiche,
- Gleissperre,
- Hauptsignal,
- Zusatzsignal“ (/5/, Seite 7).

Tabelle 8-11: Verhältnis der Stelleinheiten zu Stellwerken (nach /5/, Seite 8)

| Stellwerkstechnik | Anzahl Stelleinheiten |
|-------------------|-----------------------|
| Mechanisch | 14 |
| Elektromechanisch | 31 |
| Relais | 77 |
| ESTW | 236 |

Dabei bleibt jedoch unklar, wie der prozentuale Anteil der Signale und Weichen innerhalb der Stelleinheiten ist. In der Regel werden mehr Signale als Weichen angesteuert, so dass beispielsweise ein Anteil von 40% Weichen und 60% Signale angenommen werden kann. Für ein ESTW wären dies ca. 94 Weichen und ca. 142 Signale pro Stellwerk.

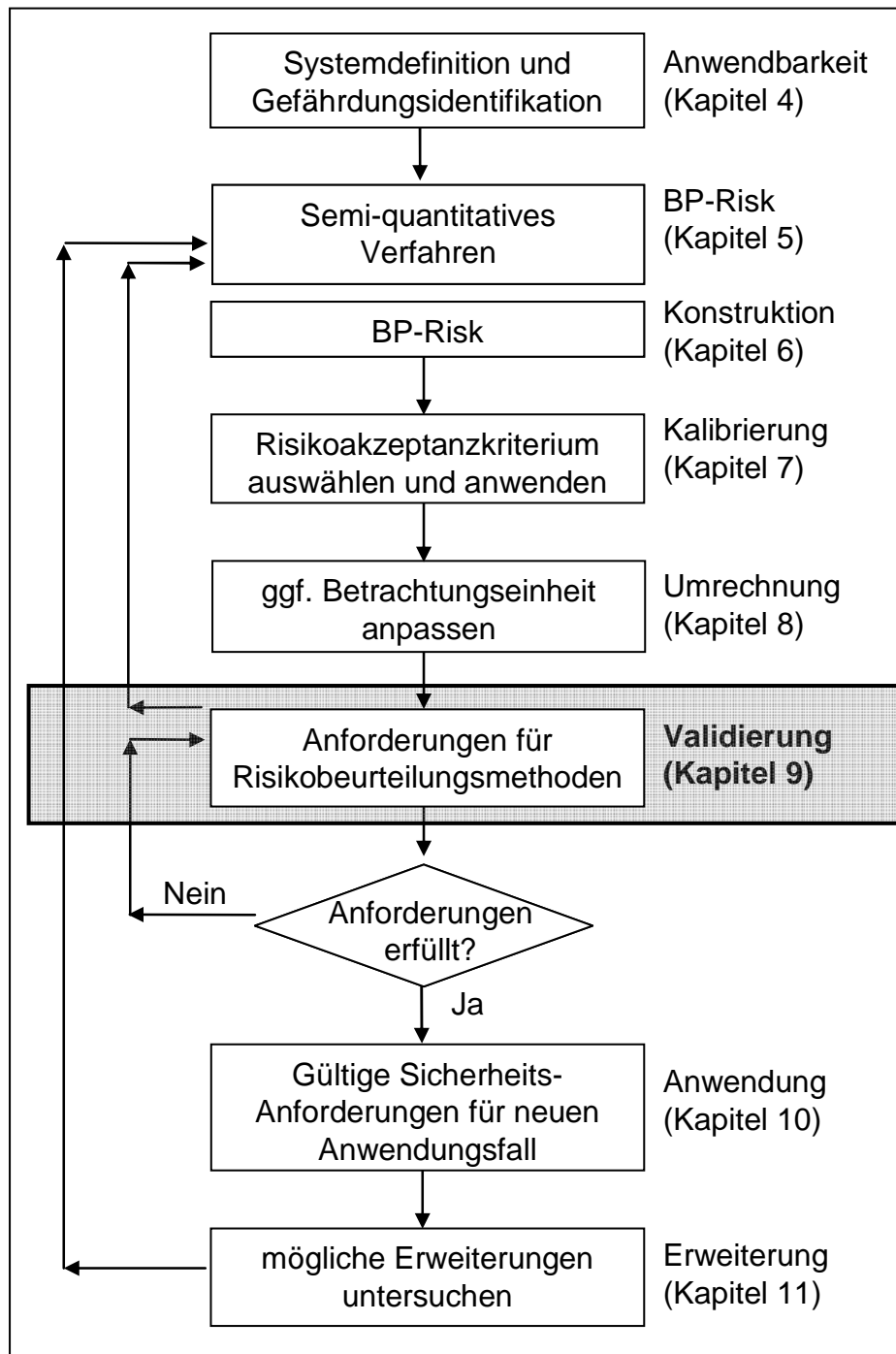
Es wird jedoch deutlich, dass eine pauschale Berücksichtigung der angesteuerten Elemente nicht sinnvoll ist, da die Werte stark von der technischen Lösung abhängen, die eher im Rahmen einer betrieblichen Ursachenanalyse berücksichtigt werden sollten.

8.4 Zusammenfassung

BP-Risk liefert Ergebnisse für Systemfunktionen anhand der Betrachtung eines Zuges. Um Funktionen an den Schnittstellen eines Zuges bewerten zu können, ist ggf. ein Wechsel der Bezugsgröße notwendig. Eine solche Umrechnung wurde mithilfe eines generischen Fehlerbaums und anhand von Umrechnungsfaktoren beispielhaft gezeigt. Dabei ist zu beachten, dass die Annahmen, die hier getroffen wurden, nur für die beispielhaften Anwendungsfälle gelten. Diese Entscheidungen gehören in der Regel zur Designfreiheit des Anwenders, der anhand eigener Kriterien die jeweiligen Versagenshäufigkeiten aufteilen und umrechnen kann.

Als Ergebnis kann festgestellt werden, dass es im Rahmen von BP-Risk nicht sinnvoll ist, einen pauschalen Umrechnungsfaktor für einen bestimmten Funktionstyp einzuführen, um die Versagenshäufigkeiten umzurechnen, da die Aufteilungen zu stark von der gewählten Systemarchitektur abhängt. Eine Gefährdungsrate in Abhängigkeit eines Streckenelements kann bislang nicht generisch bewertet werden, sondern macht es nötig, streckenspezifische Randbedingungen zu berücksichtigen. Die Einbeziehung der Anzahl der Streckenelemente widerspricht dem eigentlichen generischen Ansatz, da bislang die Umrechnung nur in Abhängigkeit von Komponenten erfolgen kann. Hier ergibt sich ein generelles Problem, da der Bezug auf eine Funktion zwar generisch, bei Streckenfunktionen jedoch nicht praktikabel ist. Bestimmte Streckenelemente werden als Komponenten und nicht pro Funktion oder pro Streckenkilometer vertrieben und müssen folglich anders bewertet werden.

Bislang ist es nicht gelungen, eine vollkommen generische Umrechnung für Streckenelemente zu konstruieren, wie sie im bereits veröffentlichten Ansatz von BP-Risk (/11/, Seite 97ff) angesetzt wurde. In diesem Kapitel wurde jedoch versucht, eine Art Kompromisslösung aufzuzeigen, die zwar die Anzahl der Streckenelemente berücksichtigt, dies jedoch möglichst ‚generisch‘ mit Hilfe der Klassifizierung durch die Streckenstandards. Damit ist zwar eine endgültige Lösung nicht gefunden, aber eine Grundlage für weitere Forschungsaktivitäten geschaffen worden.



9 Validierung

Validierung oder Validation bezeichnet in der Statistik eine Gültigkeits- oder Plausibilitätsprüfung. Diese kann sich auf Werte oder Tests beziehen. Bei einer Plausibilitätsprüfung wird ein Wert oder allgemein ein Ergebnis überschlagsmäßig daraufhin überprüft, ob es überhaupt plausibel, also annehmbar, einleuchtend und nachvollziehbar ist. In der Softwaretechnik bezeichnet Validierung (auch Test der Plausibilität) die Kontrolle eines konkreten Wertes im Hinblick darauf, ob er zu einem bestimmten Datentyp gehört oder in einem vorgegebenen Wertebereich oder einer vorgegebenen Wertemenge liegt. Die Validierung ist ein wichtiger Aspekt der Qualitätssicherung, der sicherstellen soll, dass ein implementiertes Programm den vorher aufgestellten Anforderungen genügt. Der Begriff Validierung wird oft mit dem Begriff Verifikation gleichgesetzt, obwohl in manchen Bereichen die Bedeutung eine andere ist. In der Regel wird in der Verifikation überprüft, ob ein System seiner formalen Spezifikation genügt.

Die Validierung umfasst somit zwei Aspekte:

- Prüfung, ob Anforderungen in sich korrekt sind, und
- Prüfung der Methode gegen die aufgestellten Anforderungen.

Im Folgenden wird im Rahmen der Validierung von BP-Risk insbesondere auf den zweiten Aspekt eingegangen, nämlich die Prüfung der Methode gegen die bereits in Kapitel 5.1 genannten Anforderungen für Risikobeurteilungsmethoden.

9.1 Validierung von BP-Risk

Validierung ist nach EN 50126 die „Bestätigung durch Überprüfung und objektiven Nachweis, dass die besonderen Anforderungen für einen spezifischen, bestimmungsgemäßen Gebrauch erfüllt wurden“ (/28/).

Im Zusammenhang mit dem V-Modell aus der EN 50126 wird die Validierung der Anforderungsdefinition bzw. dem Abnahmetest zugeordnet. Insofern ist im Rahmen dieser Arbeit unter der Validierung die Überprüfung der Eignung der Anforderungsdefinition mit den ursprünglichen Zielen des Kunden zu verstehen. In Abbildung 9-1 wird das Prinzip des V-Modells auf BP-Risk angewendet. Die ‚Spezifikation‘ für BP-Risk besteht somit aus den in Kapitel 5.1 vorgestellten Anforderungen aus Vorschriften und Praxis. Diese Anforderungen wurden genutzt, um das Risikomodell (siehe Kapitel 5.3), was BP-Risk zugrunde liegt, aufzustellen. Nach der mathematischen Transformation (siehe Kapitel 5.4) dieses Modells folgte das eigentliche ‚Produkt‘, nämlich die BP-Risk-Tabellen (siehe Kapitel 6), deren Anwendung in dieser Arbeit (oder zukünftig in einem Nutzerhandbuch) beschrieben wird.

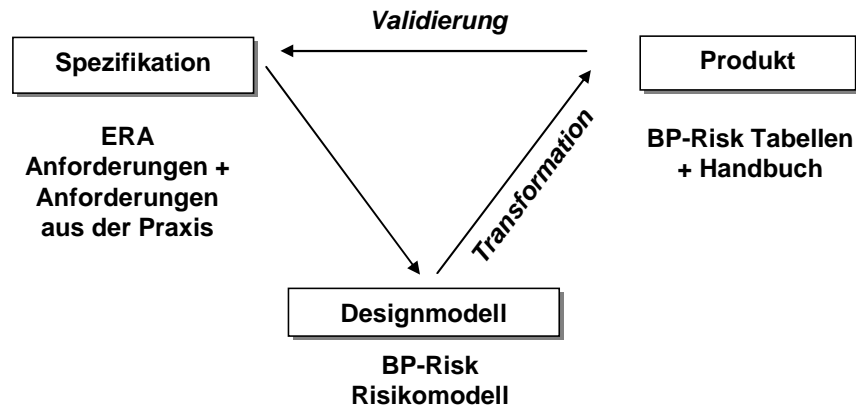


Abbildung 9-1 Validierung von BP-Risk

Die folgende Validierung überprüft nun, ob die BP-Risk-Methode die Anforderungen der Spezifikation erfüllt, und kontrolliert somit indirekt die Korrektheit der Modellierung sowie der Transformation. Es ist nicht Gegenstand der vorliegenden Validierung, alle Anforderungen der Phase Risiko- und Gefährdungsanalyse zu betrachten. Es werden nur die Anforderungen betrachtet, die unmittelbar auf die vorgelegte Methodik BP-Risk anwendbar sind. Dies betrifft in erster Linie die Beurteilung der Angemessenheit der Methode sowie deren Gültigkeit. Tabelle 9-1 stellt noch einmal die genannten Anforderungen aus Kapitel 5.1 zusammen.

Tabelle 9-1 Anforderungen für BP-Risk

| Nr. | Anforderung |
|-----|---|
| A01 | Risikoakzeptanz: keine höheren Risiken als RAC-TS |
| A02 | Implizites Restrisiko |
| A03 | Mensch und Technik-Modell |
| A04 | Unabhängige Bewertung der Systemfunktionen (hohe Systemebene) |
| A05 | Qualitative Schadens- und Folgenanalyse |
| A06 | Berücksichtigung aller relevanten Parameter |
| A07 | Genauigkeit innerhalb einer Zehnerpotenz |
| A08 | Rigoreuse Begründung der Methode; umfassende und überprüfbare Dokumentation |
| A09 | Ergebnisse: gleiches Format wie Sicherheitsziel |
| A10 | Fähigkeit, verschiedene Parameter auszugleichen |

Eine Anforderung ist im Allgemeinen eine Eigenschaft, die erfüllt sein muss, damit ein Vorgang gelingen kann. Anforderungen sind demnach geforderte Eigenschaften. Beim Sicherheitsmanagement werden Anforderungen an Systeme gestellt, damit die entsprechenden Schutzziele erreicht werden können.

Im Folgenden wird nachgewiesen, dass BP-Risk die in Tabelle 9-1 genannten Anforderungen theoretisch erfüllt. Ein praktischer Nachweis erfolgt durch das neue Anwendungsbeispiel in Kapitel 10.

9.2 Anforderung A01

| Nr. | Anforderung |
|-----|---|
| A01 | Risikoakzeptanz: keine höheren Risiken als RAC-TS |

Einer der wichtigsten Erfahrungen und Erkenntnisse aus /9/ (Seite 94) besagt, dass der glaubwürdigste und effizienteste Ansatz zur Risikoakzeptanz die Forderung gleicher Sicherheit nach GAMAB oder MGS ist. Daher wurde das MGS – Prinzip als Risikoakzeptanzkriterium in die allgemeinen Anforderungen an eine effiziente Risikobeurteilungsmethode für die Eisenbahntechnik aufgenommen.

Im Rahmen der ERA-Arbeitsgruppe zum Thema Common Safety Methods wurde von der Industrie jedoch vorgeschlagen, dass bei der Anwendung der jeweiligen Methode keine höheren Risiken, als vom RAC-TS Kriterium zugelassen, akzeptiert werden sollen. Insofern kann der Nachweis von MGS entfallen, da es zukünftig keine höheren Anforderungen als RAC-TS geben kann. Dieser Aspekt findet sich in der bereits vorhandenen Normung (EN 50129) wieder, nach der eine schärfere Anforderung als $10^{-9}/h$ an keine einzelne Sicherheitsfunktion gestellt werden sollte. Diese Praxis deckt sich ebenfalls mit der aus IEC 61508 sowie einschlägigen Luftfahrtnormen (SAE-ARP 4754).

RAC-TS wurde für die Kalibrierung (siehe Kapitel 7) von BP-Risk verwendet, da es ein einheitliches europäisches Risikoakzeptanzkriterium darstellt, was speziell für explizite Risikobeurteilungsmethoden als Referenzpunkt genutzt werden kann. Da RAC-TS als Risikoakzeptanzkriterium in der ERA CSM-Recommendation verankert ist und diese im Jahre 2010 Gesetzescharakter erlangen wird, würde außerdem im Falle des Nachweises der Risikoakzeptanz europäisches über deutschem Recht stehen. Insofern erfüllt BP-Risk schon jetzt europäisches Recht, da es RAC-TS als Kalibrierungspunkt implementiert hat.

9.3 Anforderung A02

| Nr. | Anforderung |
|-----|-----------------------|
| A02 | Implizites Restrisiko |

Die Anforderung A02 ist eher eine Erklärung als eine Anforderung, da es in vielen Ländern rechtliche und moralische Bedenken gegen explizite Festlegungen von Grenzkrisen gibt. Viele Menschen fühlen sich wohler, wenn beispielsweise das Restrisiko ‚Anzahl erwarteter Todesfälle pro Jahr‘ nicht explizit ausgewiesen wird oder der ‚Wert eines verhinderten Todesfalls‘ (wie z. B. in ALARP) vermieden wird. Aus Sicht der Normen und Standards sind diese Angaben nicht erforderlich.

Weder BP-Risk, noch das Risikoakzeptanzkriterium (RAC-TS), was zur Kalibrierung von BP-Risk verwendet wird, weisen ein explizites Restrisiko aus. Im Rahmen der Kalibrierung wird statt einem Risikowert eine tolerierbare Gefährdungsrate implementiert. Dies hat den Vorteil, dass der Anwender kein Risikoakzeptanzkriterium festlegen muss.

RAC-TS ist allerdings an eine bestimmte Ebene gebunden, auf der es anwendbar ist. Daraus folgt unter anderem auch die Einhaltung einer hohen Systemebene, die sich sowohl aus der Kalibrierung als auch aus der Modellierung von BP-Risk ergibt (siehe Anforderung A04).

9.4 Anforderung A03

| Nr. | Anforderung |
|-----|---------------------------|
| A03 | Mensch und Technik-Modell |

Im Bahnwesen wurde gezeigt, dass eingeschränkte Betriebsmodi (z. B. Hilfshandlungen) oder betriebliche Rückfallebenen sehr viel gefährlicher sind als Verfahren im normalen Betrieb. In diesen Situationen spielt der Benutzer eine entscheidende Rolle. Darum müssen nicht nur bei Rückfallebenen die menschlichen Faktoren berücksichtigt werden, sondern unter anderem auch bei Wartungsverfahren. Eine Risikobeurteilungsmethode sollte sich daher nicht nur auf technische Faktoren beschränken, da nur bei der Betrachtung von Mensch und Technik Risikobeurteilungen ihre volle Wirksamkeit entfalten können.

Das Risikomodell von BP-Risk betrachtet ein System von Mensch und Technik. Die menschliche Gefahrenabwehr wird explizit durch den Parameter *M* mitberücksichtigt. Somit erfüllt BP-Risk schon per Konstruktion die Anforderung A03.

9.5 Anforderung A04

| Nr. | Anforderung |
|-----|---|
| A04 | Unabhängige Bewertung der Systemfunktionen (hohe Systemebene) |

Eine PRA („probabilistic risk analysis“) fasst oft alle Sicherheitsfunktionen zusammen und berechnet nur einen allgemeinen Risikowert. Nach den allgemeinen Anforderungen für Risikobeurteilungen sollte jedoch jede Systemfunktion unabhängig von allen anderen bewertet werden können, da die Analysen für verschiedene Funktionen entkoppelt werden.

In der Luftfahrt werden im Rahmen der FHA („functional hazard analysis“) bereits seit Jahren diese individuellen Risikobetrachtungen durchgeführt. Im Bahnsektor würden ähnliche Vorgehensweisen die Analysen um einiges vereinfachen, wie bereits mit BP-Risk aufgezeigt wurde (siehe dazu auch das Anwendungsbeispiel in Kapitel 10).

Eine derartige Entkoppelung bringt jedoch mit sich, dass Sicherheitsfunktionen auf einem hohen Systemlevel definiert werden müssen. Eine hohe Systemebene ist Voraussetzung für das BP-Risk Risikomodell, da diese die Annahme der Addition von Risiken rechtfertigt. Außerdem berücksichtigt die Kalibrierung eine hohe Systemebene durch die Anwendung von RAC-TS. Daraus ergibt sich die Betrachtungsebene für die Systemdefinition basierend auf der prEN0015380-4. Zusätzlich fordert der Ansatz von RAC-TS, „*dass jede Versagensart auf der Systemebene getrennt betrachtet wird*“ (/16/), was einer unabhängigen Bewertung der Systemfunktionen entspricht.

9.6 Anforderung A05

| Nr. | Anforderung |
|-----|---|
| A05 | Qualitative Schadens- und Folgenanalyse |

Trotz der zahlreichen Unfalldatenbanken und Prognosemodelle ist bekannt, dass die Abschätzungen der Unfallschwere und speziell die Modelle für die Folgenwahrscheinlichkeiten oft mit hohen Unsicherheiten verbunden sind. Die Anforderung A05 ergibt sich aus den Erfahrungen mit quantitativen Risikoanalysen und berücksichtigt die Erkenntnisse der Luftfahrt, in denen *„statt aller möglicher Folgen nur der schwerste glaubwürdige Unfall (nicht der schwerste vorstellbare) betrachtet“* (/9/, S. 62) und die Unfallschwere qualitativ bewertet wird.

BP-Risk führt eine qualitative Schadens- und Folgenanalyse durch, in der einheitliche Kategorien vorgegeben und verbal beschrieben werden. Durch die Einführung von Subparametern wird beispielsweise die Schadenshöhe nicht direkt geschätzt. Dies wiederum ist eine Verbesserung des Luftfahrt-Ansatzes, bei dem *„die etwas pauschale Abschätzung der Unfallschwere [...] im Vergleich zur quantitativen Folgenbewertung zu gröberen oder zu konservativen Sicherheitsanforderungen führen“* (nach /9/, Seite 63).

9.7 Anforderung A06

| Nr. | Anforderung |
|-----|---|
| A06 | Berücksichtigung aller relevanten Parameter |

Im Rahmen eines Vergleichs von verschiedenen Ansätzen zur Risikobewertung wurde die Verwendung der in der Risikoformel vorkommenden Parameter untersucht. Die Risikoformel wurde deswegen als Referenzpunkt verwendet, da zurzeit keine einfache Risikoanalysemethode bekannt ist, die mehr Parameter besitzt. Tabelle 9-2 fasst die Ergebnisse dieses Vergleichs zusammen.

Tabelle 9-2 Vergleich der Ansätze zur Risikobewertung (aus /9/, Seite 64)

| Ansatz | Parameter | | | | | |
|--------------|--------------------|----------------------------|----------------------|----------------|------------------------|--------------------|
| | Nutzungsprofil (N) | Gefährdungshäufigkeit (HR) | Aussetzungsdauer (E) | Latenzzeit (D) | Reduktionsfaktoren (C) | Schadensausmaß (S) |
| Risikoformel | + | + | + | + | + | + |
| Risikograph | 0 | 0 | 0 | - | 0 | 0 |
| Risikomatrix | 0 | 0 | - | - | - | 0 |
| RPN | - | 0 | - | - | 0 | 0 |
| Yellow Book | + | + | 0 | - | + | + |
| ASCAP | + | + | + | + | + | 0 |
| FHA | 0 | +/0 | +/0 | +/0 | +/0 | 0 |

Die Symbole haben folgende Bedeutungen:

- + Parameter wird berücksichtigt und kann differenziert werden,
- 0 Parameter vorhanden, Verwendung unterliegt aber Einschränkungen,
- Parameter wird nicht berücksichtigt.

Viele Ansätze für Risikoanalysen berücksichtigen nicht alle relevanten Parameter wie z. B. Aussetzungsdauer oder Latenzzeit. Daraus ergab sich die Anforderung, dass bei Einführung eines Risikoanalysemodells Beweise aufgeführt werden müssen, die nachweisen, dass alle relevanten Parameter einbezogen werden.

Die ERA Empfehlungen für die CSM besagen in Artikel 10 (Absatz 5), dass: *„die Methoden für die explizite Risikoeinschätzung das zu bewertende System sowie deren Parameter korrekt wieder spiegeln sollen (inklusive aller betrieblichen Modi)“* (aus dem Englischen nach /62/). Auch die bereits genannten Anforderungen der ERA-Arbeitsgruppen zum Thema Common Safety Methods fordern unter anderem, dass *„alle relevanten Parameter in Bezug auf das Eisenbahnwesen berücksichtigt werden, insbesondere:*

- *Aussetzungsdauer,*
- *Möglichkeit zur Gefahrenabwehr,*
- *Fehleroffenbarung,*
- *Schadensausmaß.“* (aus dem Englischen nach /114/).

Im Rahmen der Validierung von BP-Risk wird die Erfüllung dieser Anforderung gezeigt, indem das zugrunde liegende Risikomodell von BP-Risk, das ein kollektives Risiko betrachtet, aus der Risikoformel für individuelle Risiken abgeleitet wird. Der Ablauf des Nachweises ist dargestellt in Abbildung 9-2.

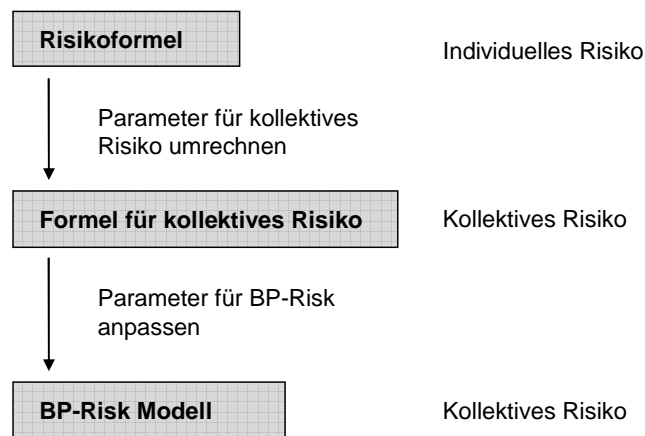


Abbildung 9-2 Ablauf des Nachweises

Ausgehend vom Risikomodell für individuelle Risiken werden im Folgenden die einzelnen Parameter für eine Betrachtung des kollektiven Risikos angepasst. Anschließend werden die Randbedingungen von BP-Risk in die abgeleitete Formel für kollektives Risiko implementiert. Abschließend wird die angepasste Risikoformel mit dem BP-Risk Risikomodell verglichen, um zu beurteilen, ob alle relevanten Parameter berücksichtigt wurden.

9.7.1 Risikoformel für individuelles Risiko

Die Risikoformel dient der allgemeinen Bewertung individueller Risiken. Die in der Risikoanalyse nach EN 50129 vorkommenden Prozessschritte sowie die benötigten Parameter werden dabei in generischer Form berücksichtigt; siehe hierzu /20/. Eine ausführliche Begründung der Formel, deren Parameter sowie einige Erweiterungen finden sich in /22/. Das individuelle Risiko für einen Todesfall IRF_i wird in der Risikoformel definiert durch Gl. 9-1:

| | | |
|--|--|---------|
| $IRF_i = N_i \sum_{j=1}^n (HR_j D_j + HR_j E_{ij}) \sum_{k=1}^q (C_{jk} F_{ik})$ | | Gl. 9-1 |
| i | Index des Individuums I_i mit $I_i \in I = \{I_i \mid i = 1, \dots, m\}$ [-] | |
| IRF_i | Individuelles Risiko eines Todesfalls des Individuums I_i [Wahrscheinlichkeit eines Todesfalls pro Zeiteinheit] | |
| N_i | Benutzerprofil des Individuums I_i (Anzahl der Verwendungen durch Individuums I_i) [1/Zeiteinheit] | |
| j | Index der Gefährdung H_j mit $H_j \in H = \{H_j \mid j = 1, \dots, n\}$ [-] | |
| HR_j | Gefährdungsrate für jeweilige Gefährdung H_j [1/Zeiteinheit] | |
| D_j | Latenzzeit (Gefährdungsdauer) der Gefährdung H_j [Zeiteinheit] | |
| E_{ij} | Zeit, die Individuums I_i der Gefährdung H_j ausgesetzt ist (Aussetzungsdauer) [Zeiteinheit] | |
| k | Index des Unfalls vom Typ A_k mit $A_k \in A = \{A_k \mid k = 1, \dots, q\}$ [-] | |
| C_{jk} | Folgenwahrscheinlichkeit für Gefährdung H_j und Unfall A_k (Risikoreduktionsfaktoren) [-] | |
| F_{ik} | Wahrscheinlichkeit eines Todesfalls des Individuums I_i für Unfalltyp A_k (Schweregrad) [-] | |

9.7.2 Formel für kollektives Risiko

Im Rahmen einer Risikobeurteilung im Eisenbahnwesen handelt es sich bei den betrachteten Personengruppen in der Regel um Reisende. Dabei unterliegt meist die Annahme, dass, wenn der Reisende hinreichend geschützt wird, die anderen Rechtsgüter (Bahnmitarbeiter, Anwohner, Straßenverkehrsteilnehmer, Sachwerte, Umwelt, u. a.) ebenfalls hinreichend geschützt sind (siehe auch Kapitel 6.2). Dieser Argumentation folgend, wird für das kollektive Risiko nun nicht mehr ein Individuum betrachtet, sondern ein Kollektiv – in diesem Fall ein Zug Z_i ($i = 1, \dots, m$) mit mehreren Reisenden und Bahnpersonal als Insassen. Das Risiko wird somit nicht mehr auf einen einzelnen Menschen umgerechnet, sondern auf einen Zug. Daher werden nur noch die Unfälle berücksichtigt, die den Zug betreffen – also Schaden am Zug anrichten. Unfälle, die Personenschäden, aber keinen Schaden am Zug verursachen (z. B. Person klemmt sich in der Tür), werden ggf. in einer Erweiterung des BP-Risk Ansatzes berücksichtigt. Siehe dazu Kapitel 11.1. Analog zum individuellen Risiko ist bei der Benutzung des Systems der Zug Gefährdungen H_j ausgesetzt, die aus Versagen von Systemfunktionen (oder Teilfunktionen) entstehen. Dies wird durch eine Liste von Gefährdungen und entsprechenden Gefährdungsraten (H_j, HR_j) beschrieben.

Vereinfachend wird für das kollektive Risiko eine Reisedauer von einer Stunde Dauer $E_i = 1h = \text{const.}$ angenommen. In der Regel fahren Personenzüge tagsüber häufiger als nachts – bei Güterzügen ist es umgekehrt. Das Modell macht dabei keinen Unterschied, sondern nimmt an, dass der Zug (unabhängig ob Personen- oder Güterzug) zu einem zufälligen Zeitpunkt das System betritt. Da die vorgegebene Bezugsgröße $E_i = 1h$ angenommen wird, folgt für das Benutzerprofil (Zahl der Verwendungen) $N_i = 1/h = \text{const.}$ Anders ausgedrückt bedeutet dies, dass der betrachtete Zug Z_i das System Eisenbahnbetrieb ein einziges Mal für eine Stunde benutzt.

Entsprechend der Risikoformel ist die Wahrscheinlichkeit, dass der Zug Z_i einer Gefährdung H_j begegnet, abhängig von der Gefährdungsdauer D_j und der Zeit E_{ij} , die der Zug der Gefährdung H_j ausgesetzt ist. Nach /9/ (Seite 38ff) schützt die Berücksichtigung des Parameters D_j vor latenten Gefährdungen und zwingt dazu, entweder Gefährdungen explizit zu offenbaren oder ihre Auftretenshäufigkeit extrem zu reduzieren. Auf den Aspekt der Gefährdungsdauer wird im Rahmen der Anpassung der kollektiven Risikoformel für BP-Risk noch einmal genauer eingegangen.

Durch die Folgewahrscheinlichkeit C_{jk} wird wie beim individuellen Risiko beschrieben, wie sich aus einer Gefährdung H_j ein Unfall oder mehrere Unfälle A vom Typ k ergeben können. Diese Wahrscheinlichkeit berücksichtigt also die externen Risikoreduktionsfaktoren, z. B. menschliche Gefahrenabwehr. Für das kollektive Risiko wird nun nicht mehr die Wahrscheinlichkeit betrachtet, dass ein Individuum bei einem Unfall stirbt, sondern ein kollektiver Schweregrad, genannt Schadenspotenzial S_{ik} für den betrachteten Zug Z_i und den jeweiligen Unfalltyp A_k .

Zusammenfassend kann somit das kollektive Risiko für den betrachteten Zug Z_i mit folgender Formel (Gl. 9-2) beschrieben werden:

| | | |
|---|--|----------------|
| $KR_i = \sum_{j=1}^n (HR_j D_j + HR_j E_{ij}) \sum_{k=1}^q (C_{jk} S_{ik})$ | | Gl. 9-2 |
| i | Index des Zugs Z_i mit $Z_i \in Z = \{Z_i \mid i = 1, \dots, m\}$ [-] | |
| KR_i | Kollektives Risiko für Zug Z_i [Opfer pro Zugstunde] | |
| j | Index der Gefährdung vom Typ H_j mit $H_j \in H = \{H_j \mid j = 1, \dots, n\}$ [-] | |
| HR_j | Gefährdungsrate für jeweilige Gefährdung H_j [1/h] | |
| D_j | Latenzzeit (Gefährdungsdauer) der Gefährdung H_j [Zeiteinheit] | |
| E_{ij} | Zeit, die der Zug Z_i der Gefährdung H_j ausgesetzt ist (Aussetzungsdauer) [Zeiteinheit] | |
| C_{jk} | Folgewahrscheinlichkeit für Gefährdung H_j und Unfall A_k (Risikoreduktionsfaktoren) [-] | |
| k | Index des Unfalls vom Typ A_k mit $A_k \in A = \{A_k \mid k = 1, \dots, q\}$ [-] | |
| S_{ik} | Schadensausmaß für Zug Z_i und jeweiligen Unfall A_k [Opfer] | |

Anpassung für BP-Risk

Der Grundansatz von BP-Risk besteht darin, dass für jede Systemgefährdung eine vereinfachte Folgen- und Schadensabschätzung des zugehörigen Szenarios durchgeführt wird. Somit entfällt die Summe der Gefährdungen H_j in der Formel für das kollektive Risiko, da BP-Risk für jede Systemgefährdung eine eigene Risikoabschätzung durchführt. In der Formel entfällt ebenso die Summe über die Unfälle A_k , da der schwerste, jedoch noch glaubwürdigste Schadensfall, mit dem größten Risikowert bei BP-Risk eingeht. Betrachtet wird ein realistisches Unfallszenario (mit zugehörigen Reduktionsfaktoren und Schadenspotenzial), statt die Summe der verschiedenen Produkte aus Unfallwahrscheinlichkeit und Unfallschwere zu bilden. Würde man diese Zusammenhänge in einem Ereignisbaum darstellen, bedeutet dies, dass man nur einen Pfad des Ereignisbaums berücksichtigt (siehe Abbildung 9-3).

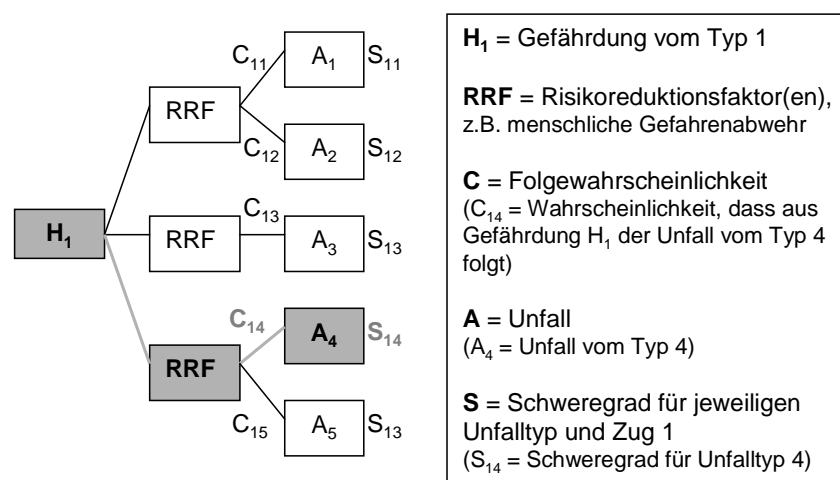


Abbildung 9-3 Von der Gefährdung zum Unfall

Wichtig dabei ist, dass man bei qualitativen Beurteilungen nicht den ‚worst-case‘-Pfad annehmen sollte, da dadurch zu konservative Ergebnisse erzielt werden. Es ist also darauf zu achten, den schwersten, aber noch glaubwürdigsten Schadensfall in der Risikobetrachtung zu bewerten. Bei zwei gleichschweren Unfällen (gleich hoher Risikowert) müsste ggf. die resultierende THR durch die Anzahl der gleichwertigen Unfälle geteilt werden, so dass eine schärfere Anforderung entsteht. Dies ist allerdings ein theoretischer Fall, da es durch die vorgegebene Konstruktion von BP-Risk kaum möglich ist, zwei gleichschwere Unfälle mit gleichem Risikowert zu erhalten. Die meisten Risikoparameter sind schon durch die betrieblichen Randbedingungen des Gefährdungsszenarios festgelegt.

Die Zeit, die der Zug Z_i der Gefährdung H_j ausgesetzt ist, hängt von der Fehlerlatenzzeit D_j und der Dauer der Zugfahrt E_i ab. Da die Gefährdungsrate HR_j dauerhaft anliegt, wird zur sicheren Seite die Aussetzungsdauer dem Betrachtungszeitraum gleichgesetzt, also $E_{ij} = E_i = 1h$. Diese Abschätzung gilt für das kollektive Risiko, wenn ein Zug betrachtet wird, also für Fahrzeugfunktionen. Bei der Betrachtung von Streckenfunktionen wird der Parameter E_{ij} implizit berücksichtigt, wenn darunter die Einwirkung von Streckenelementen auf den Zug verstanden werden kann, also z. B. wie häufig ein Zug einem Streckenelement begegnet bzw. von diesem beeinflusst wird.

Die Berücksichtigung des Parameters D_j soll vor latenten Gefährdungen schützen. In Kapitel 5.3.1 wurde bereits auf die Rolle der Gefährdungsdauer im Rahmen von BP-Risk eingegangen und deutlich gemacht, dass die Berücksichtigung der Gefährdungsdauer im Bereich der Gefahrenabwehr nicht sinnvoll ist. Bei der Betrachtung von streckenseitigen Funktionen ist die Gefährdungsdauer nur dann relevant, wenn die Gefährdung durch einen anderen Zug offenbart werden kann, was unter anderem von der Zugfolge abhängig ist. Da der Umrechnungsfaktor für den Wechsel der Bezugsgröße auf Streckenkilometer mit Hilfe der Auslastung (Zug pro Zeiteinheit) berechnet werden kann, besteht damit auch eine Abhängigkeit zur streckenseitigen Gefährdungsdauer (siehe Tabelle 5-3). Implizit wird die Gefährdungsdauer also durch den Umrechnungsparameter u berücksichtigt, wenn sie, wie oben angenommen, für Streckenfunktionen von der Betriebsdichte abhängt.

Das kollektive Risiko KR_{ijk} für BP-Risk kann dann mit folgender Formel (Gl. 9-3) ausgedrückt werden:

| | | |
|---|---|----------------|
| $KR_{ijk} = HR_j \cdot C_{jk} \cdot S_{ik}$ | | Gl. 9-3 |
| i | Index des Zugs Z_i mit $Z_i \in Z = \{Z_i \mid i = 1, \dots, m\}$ [-] | |
| j | Index der Gefährdung vom Typ H_j mit $H_j \in H = \{H_j \mid j = 1, \dots, n\}$ [-] | |
| k | Index des Unfalls vom Typ A_k mit $A_k \in A = \{A_k \mid k = 1, \dots, q\}$ [-] | |
| KR_{ijk} | Kollektives Risiko für Zug Z_i , Gefährdungsszenario H_j und resultierendem Unfalltyp A_k [Opfer pro Zugstunde] | |
| HR_j | Gefährdungsrate für jeweilige Gefährdung H_j [1/h] | |
| C_{jk} | Folgenwahrscheinlichkeit für Gefährdung H_j und Unfall A_k (Risikoreduktionsfaktoren) [-] | |
| S_{ik} | Schadensausmaß für Zug Z_i und jeweiligen Unfall A_k [Opfer] | |

Diese Formel ähnelt der in /9/ hergeleiteten angepassten Formel für die Functional Hazard Analysis (FHA) aus der zivilen Luftfahrt: $R_j = HR_j \cdot D_j \cdot C_j \cdot S_j$ (/9/, Seite 62), wobei anzumerken ist, dass die Bestehenszeit der Gefährdung D_j sowie die Reduktionsfaktoren C_j nur in der Ursachenanalyse (PSSA) vorkommen.

Beim Vergleich der FHA mit der kollektiven Risikoformel für BP-Risk erkennt man starke Analogien:

- in der FHA wird ein Gesamtsystem ‚Flugzeug‘ betrachtet, bei BP-Risk ein ‚Zug‘;
- bei beiden Ansätzen bildet die Grundlage das kollektive Risiko;
- die Risiken werden für jede Gefährdung separat bewertet;
- es wird eine feste Missionsdauer, also eine Flugstunde bzw. Zugstunde angesetzt;
- es wird statt aller möglichen Folgen nur der schwerste, glaubwürdigste Unfall angenommen;
- das Risikoakzeptanzkriterium ist bei der FHA in der Luftfahrt international abgestimmt, für BP-Risk ist ein in der europäischen Gesetzgebung verankertes Risikoakzeptanzkriterium implementiert.

9.7.3 BP-Risk Model

Wie bereits in Kapitel 5.3 beschrieben, kann das Teilrisiko für eine Systemgefährdung im Rahmen des BP-Risk Ansatzes ausgedrückt werden durch die Formel:

$$R_i = f_i \cdot g_i \cdot s_i$$

Abbildung 9-4 illustriert, wie diese Parameter mit den Parametern aus der oben aufgestellten kollektiven Risikoformel korrespondieren.

$$KR_{ijk} = HR_j \cdot C_{jk} \cdot S_{ik}$$

$$R_i = f_i \cdot g_i \cdot s_i$$

Abbildung 9-4 kollektives Risiko und BP-Risk Risikomodell im Vergleich

Das kollektive Risiko KR_{ijk} für einen Zug Z_i , ein Gefährdungsszenario H_j und dem dazugehörigen typischen Unfalltyp A_k entspricht dem Teilrisiko R_i einer Systemgefährdung. Die Gefährdungsrate HR_j entspricht der Auftretenshäufigkeit f_i dieser Systemgefährdung. Die Risikoreduktionsfaktoren, repräsentiert durch C_{jk} , werden durch den Parameter Gefahrenabwehr g_i berücksichtigt. Das kollektive Schadensausmaß S_{ik} entspricht dem Parameter s_i in BP-Risk. Die Fehlerlatenzzeit D_j sowie die Aussetzungsdauer E_{ij} finden sich implizit in der weiterführenden Umrechnung wieder, die insbesondere für die Betrachtung von Streckenfunktionen verwendet wird. Tabelle 9-3 stellt die von der ERA geforderten relevanten Parameter den BP-Risk Parametern gegenüber und zeigt somit, dass die Methode diese berücksichtigt.

Tabelle 9-3 Relevante Parameter bei BP-Risk

| Relevanter Parameter | BP-Risk |
|--------------------------------|-----------------------------------|
| Möglichkeit zur Gefahrenabwehr | Parameter G |
| Schadensausmaß | Parameter S |
| Aussetzungsdauer | Einwirkung auf den Zug (implizit) |
| Fehleroffenbarung | Gefährdungsdauer (implizit) |

Mit der Annahme, dass die Risikoformel alle relevanten Parameter in Bezug auf das Eisenbahnwesen beinhaltet, kann mit der Herleitung des kollektiven Risikos aus der Risikoformel die oben genannte Anforderung für BP-Risk nachgewiesen werden (siehe auch /87/).

Es hat sich gezeigt, dass die Berücksichtigung der Aussetzungsdauer und der Fehleroffenbarung nicht für jedes Risikomodell sinnvoll ist. Somit ist zu klären, ob die Anforderung für alle Risikobeurteilungsmethoden zwingend erforderlich ist und sie nicht auch abgeschwächt werden könnte, wenn gezeigt werden kann, dass bei der Aufstellung des zugrunde liegenden Modells die Aspekte der Aussetzungsdauer und der Fehleroffenbarung mit bedacht wurden.

9.8 Anforderung A07

| Nr. | Anforderung |
|-----|--|
| A07 | Genauigkeit innerhalb einer Zehnerpotenz |

Risikobeurteilungen werden oft als objektiv angesehen und deren Ergebnisse in Form von Risikowerten sowie die Entscheidungen, die darauf basieren, werden als korrekt angenommen. Denn es *„bemühen sich nur wenige probabilistische Risikoanalysen darum, die Genauigkeit oder die Relevanz der Daten zu verifizieren, die sie benutzen, um die Wahrscheinlichkeit von zukünftigen Ereignissen aus vergangenen Vorfällen zu prognostizieren“* (aus dem Englischen nach /103/). Alle Schritte des Prozesses, inklusive der angewendeten Methode, sind subjektiv. Es gibt immer Unsicherheiten, menschliche Fehleinschätzungen sowie Ungenauigkeiten. Es ist unwahrscheinlich, dass verschiedene Analysten, die mit der gleichen Information ihre Analyse durchführen auch die exakt gleichen Ergebnisse erhalten. Die Zukunft besitzt ein implizites Risiko, das jedoch kein gegenwärtiges Problem beschreibt. Sie besitzt keine zukünftige Gewissheit, sondern lediglich ein Potenzial für einen zukünftigen Schaden. Somit kann ein Risiko zwar geschätzt, jedoch nicht gemessen oder berechnet werden, noch kann angenommen werden, dass die erhaltenen Risikowerte korrekt sind (nach /101/).

Um diese menschlichen Fehleinschätzungen sowie Ungenauigkeiten zu begrenzen, schreibt die ERA vor, dass *„die Ergebnisse ausreichend präzise [sein sollen], um als solide Entscheidungshilfe dienen zu können, d. h. dass geringfügige Änderungen bei zu Grunde gelegten Annahmen oder Voraussetzungen nicht zu erheblichen Unterschieden bei den Anforderungen führen“* (/59/, Artikel 10).

Für effiziente Verfahren zur Risikoanalyse schlägt die UNIFE vor, dass die Genauigkeit von quantitativen Ergebnissen innerhalb einer Zehnerpotenz liegen soll. Diese Anforderung stammt aus Erfahrungen mit Ungenauigkeiten in PRAs, in denen eine Zehnerpotenz ein angemessenes Genauigkeitsziel ist. Unter anderem wird dadurch beachtet, dass qualitative bzw. semi-quantitative Ansätze Rundungsfehler berücksichtigen müssen. Außerdem begründet es die herkömmliche Praxis der SIL⁵⁷ Ableitung. Sobald ein SIL-Wert abgeleitet wurde, muss gezeigt werden, dass die quantitative Anforderung die beschriebene Zehnerpotenz erfüllt. Diese Anforderung wird ebenfalls aus der Praxis bestätigt, die annimmt, *„dass die Ungenauigkeit einer Risikoanalyse allgemein auf eine oder zwei Größenordnungen geschätzt wird“* (/81/).

Unsicherheitsanalysen für Probabilistische Sicherheitsanalysen (PSA) gehören nach internationaler Praxis auch in anderen Industriezweigen (z. B. Kernkraft) zum Stand der Wissenschaft und Technik und sind entsprechend den folgenden Ausführungen in der PSA durchzuführen:

⁵⁷ SIL: Safety Integrity Level (Sicherheitsanforderungsstufe).

„Es ist inzwischen international üblich, in der probabilistischen Modellierung zwischen aleatorischen⁵⁸ und epistemischen⁵⁹ Unsicherheiten zu unterscheiden. Die epistemische Unsicherheit ergibt sich aus der unvollständigen Kenntnis über den zu modellierenden Vorgang. Demgegenüber wird unter der aleatorischen Unsicherheit der zufallsbedingte Charakter des modellierten Experiments bzw. Prozesses verstanden. In der PSA sind die epistemischen Unsicherheiten überwiegend den folgenden Ursachenkomplexen zuzuordnen:

- Ungewissheit über die Vollständigkeit des analysierten Ereignisspektrums,
- Abweichungen zwischen der Realität und der (vereinfachten) Modellierung der realen Prozesse,
- Begrenzte Erfahrungsgrundlage bei der Quantifizierung von Zuverlässigkeitskenngrößen, insbesondere bezüglich der Übertragbarkeit von Betriebserfahrungen“ (/23/).

Es gibt dementsprechend zwei Fehlerarten, die die Genauigkeit einer Risikobeurteilungsmethode bestimmen: Einschätzungsfehler (Ef) vom Benutzer sowie Rundungsfehler (Rf) aufgrund der Konstruktion des Verfahrens.

Die Anforderung A07 an qualitative oder semi-quantitative Verfahren lautet, dass die Genauigkeit innerhalb einer Zehnerpotenz liegen soll. Dies bedeutet für die Ableitung von zulässigen Versagenshäufigkeiten, dass eine ermittelte Gefährdungsrate sich bei unabhängigen Anwendern maximal um eine Zehnerpotenz unterscheiden darf. In der Häufigkeitstabelle von BP-Risk würde eine Zehnerpotenz immer zwei Skalenpunkten entsprechen – ein Skalenpunkt Abweichung nach oben oder nach unten (siehe Tabelle 9-4).

Tabelle 9-4 Zehnerpotenz in der Häufigkeitstabelle

| THR | G + S + U | Beschreibung | Zehnerpotenz |
|-----------------------|-----------|----------------------------|--------------|
| $3 \cdot 10^{-9} /h$ | 23 | Einmal in 30.000 Jahren | -1 |
| $10^{-9} /h$ | 24 | Einmal in 100.000 Jahren | |
| $3 \cdot 10^{-10} /h$ | 25 | Einmal in 300.000 Jahren | +1 |
| $10^{-10} /h$ | 26 | Einmal in 1.000.000 Jahren | |
| $3 \cdot 10^{-11} /h$ | 27 | Einmal in 3.000.000 Jahren | |

So kann die Anforderung A07 in Bezug auf die beiden Fehlerarten wie folgt ausgedrückt werden (mf = mittlerer Fehler):

$$mf = |Rf + Ef| \leq 2 \quad \text{Gleichung 9-4}$$

Der Einschätzungsfehler des Benutzers kann auftreten, wenn der Anwender sich in der Einschätzung eines Parameterwertes irrt. Dieser Fehler kann in beide Richtungen erfolgen. Es kann sowohl ein zu niedriger als auch ein zu hoher Wert angenommen werden.

⁵⁸ aleatorisch = vom Zufall abhängig (/89/).

⁵⁹ epistemisch = wissend, kundig (/44/).

Beim BP-Risk Verfahren wird davon ausgegangen, dass die verbale Beschreibung der Parameterwerte so gewählt ist, dass im Mittel der Anwender sich bei höchstens einer der fünf Tabellen um einen Wert verschätzt. Dieser minimale Einschätzungsfehler kann zum einen mit der sorgfältigen Konstruktion der BP-Risk Tabellen und zum anderen mit dem Gebrauch von geläufigen Termini aus der Bahntechnik (die dem Anwender vertraut sind) begründet werden. Da die Werte in den Tabellen alle denselben Abstand haben, beträgt der Einschätzungsfehler im Mittel einem Skalenwert von $Ef = 1$. Wenn zum Beispiel die maßgebliche Geschwindigkeit in Wirklichkeit ‚hoch‘ ist und der Anwender fälschlicherweise die Geschwindigkeit auf einer Hauptstrecke mit ‚sehr hoher‘ Geschwindigkeit wählt, dann würde er statt des Parameterwert $V = 3$, den Parameterwert $V = 4$ benutzen (siehe Tabelle 9-5).

Tabelle 9-5 Einschätzungsfehler

| v (km/h) | Transf. | Beschreibung | Beispiel | Ef |
|----------|---------|--------------|----------------------------------|-------------|
| 38 | 1 | Gering | Rangieren, Fahrt auf Befehl, ... | |
| 60 | 2 | Mittel | | - 1 |
| 100 | 3 | Hoch | Neben- und Regionalstrecken | Wahrer Wert |
| 160 | 4 | Sehr Hoch | Haupt und HGV-Strecken | + 1 |

Der Rundungsfehler (Rf) erfolgt aufgrund der Konstruktion der BP-Risk Tabellen. Die logarithmierten Werte sind meist keine ganzen Zahlen. Die Differenz zu den entsprechenden ganzzahligen qualitativen Parameterwerten wird als Rundungsfehler ausgewiesen. Für den Parameter V ist dies beispielsweise die Differenz der Spalte 4 (Qualitativer Parameterwert) minus der Spalte 2 (Logarithmierter Quantitativer Wert) in Tabelle 9-6.

Tabelle 9-6 Rundungsfehler beim Parameter V

| v (km/h) | Log v^2 Basis Wurzel 10 | Rundungs- fehler (Rf) | Qualitativ V | Transf (V -5) |
|---------------|------------------------------|------------------------------|-----------------|------------------|
| 38 | 6.30 | -0.30 | 6 | 1 |
| 60 | 7.11 | -0.11 | 7 | 2 |
| 100 | 8.00 | 0.00 | 8 | 3 |
| 160 | 8.82 | 0.18 | 9 | 4 |
| Summe: | | -0.23 | | |

Es wird angenommen, dass eine zu hohe oder zu niedrige Einschätzung eines Parameters gleich wahrscheinlich ist, so dass sich nur in 50% der Fälle der Fehler zur ungünstigen Seite auswirkt - also der Einschätzungsfehler zum Rundungsfehler addiert wird. In den anderen 50% der Fälle gleichen sich die Fehler eher aus. Dabei ist zu beachten, dass im Gegensatz zum Einschätzungsfehler das Vorzeichen beim Rundungsfehler eine Rolle spielt, da dieses angibt, in welche Richtung der Fehler tendiert. Beispielsweise bedeutet eine positive Summe der Rundungsfehler für einen Parameter, dass die qualitativen Werte im Mittel immer höher sind als die logarithmierten quantitativen Werte.

Ein positiver Rundungsfehler bedeutet, dass die qualitativen Werte eher zur sicheren Seite liegen und die Anforderungen ein wenig strenger sind, als sie sein müssten. Umgekehrt würde ein negativer Rundungsfehler bedeuten, dass die Werte eher unterschätzt werden und die resultierenden Sicherheitsanforderungen damit möglicherweise zu niedrig sind. Insgesamt zeigt Abbildung 9-5 jedoch, dass der Rundungsfehler sehr ausgeglichen ist. In ca. 52% der Fälle werden die Parameterwerte abgerundet (negativer Rundungsfehler), was bedeutet, dass der logarithmierte quantitative Wert höher liegt als der gerundete qualitative Wert. Folglich werden in 48% der Fälle die Parameterwerte aufgerundet (positiver Rundungsfehler).

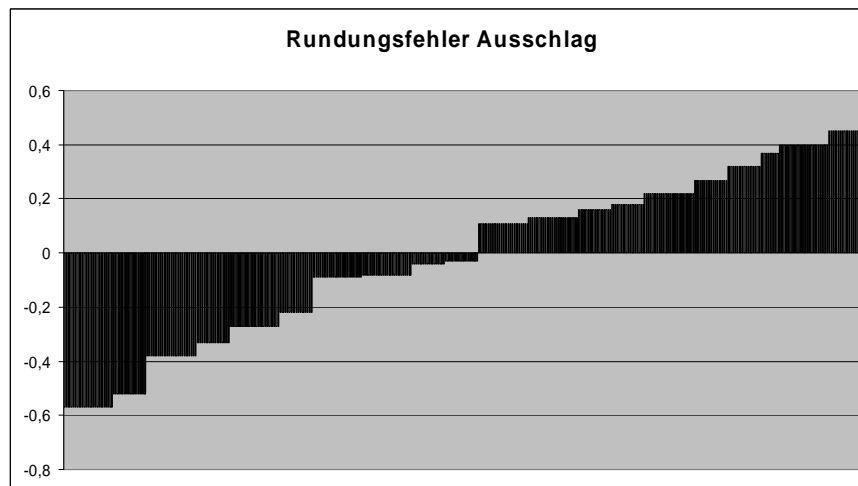


Abbildung 9-5 Rundungsfehler Ausschlag

Der Rundungsfehler von allen Parameterkombinationen ist in Abbildung 9-6 dargestellt.

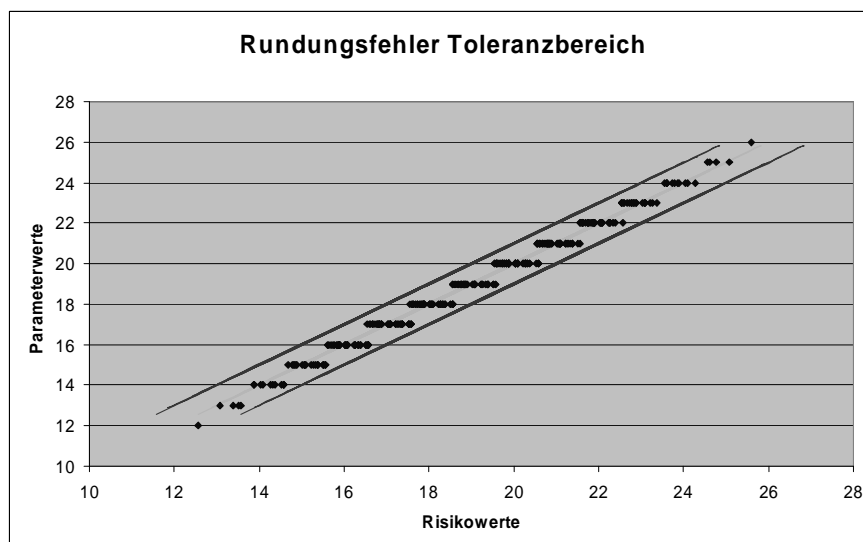


Abbildung 9-6 Rundungsfehler Toleranzbereich

Die Punkte stellen die Werte dar, die durch die Anwendung der BP-Risk Tabellen entstehen. Sie sind den hinterlegten Risikowerten des BP-Risk Risikomodells gegenübergestellt. Die dünne Linie in der Mitte stellt die quantitativen Werte ohne Rundung dar. Die äußeren Linien begrenzen den tolerierbaren Bereich des Rundungsfehlers (quantitative Werte ± 1).

Abbildung 9-6 zeigt, dass die berechneten Werte im Toleranzbereich liegen und sich jeweils ober- und unterhalb der dünnen Linie befinden. Das bedeutet in diesem Fall, dass sich die Rundungsfehler in den meisten Fällen ausgleichen. Insgesamt beträgt der durchschnittliche absolute Rundungsfehler $R_f = 0,25$ (mit einer Standardabweichung von 0,16). Der mittlere Fehler (mf) beträgt also: $mf = R_f + E_f = 0,25 + 1,00 = 1,25 \leq 2,00$ und erfüllt somit die Anforderung A07.

Allerdings berücksichtigt diese Rechnung nur den mittleren Rundungsfehler. Es sind jedoch auch Kombinationen möglich, bei denen systematisch größere Abweichungen vorkommen. Die maximalen Werte des Rundungsfehlers betragen den Wert 0,57, so dass der mittlere Fehler für diese maximalen Werte immer noch die Anforderung erfüllt, da $mf = R_{f_{max}} + E_f = 0,57 + 1,00 = 1,57 \leq 2,00$ (siehe dazu auch Abbildung 9-7).

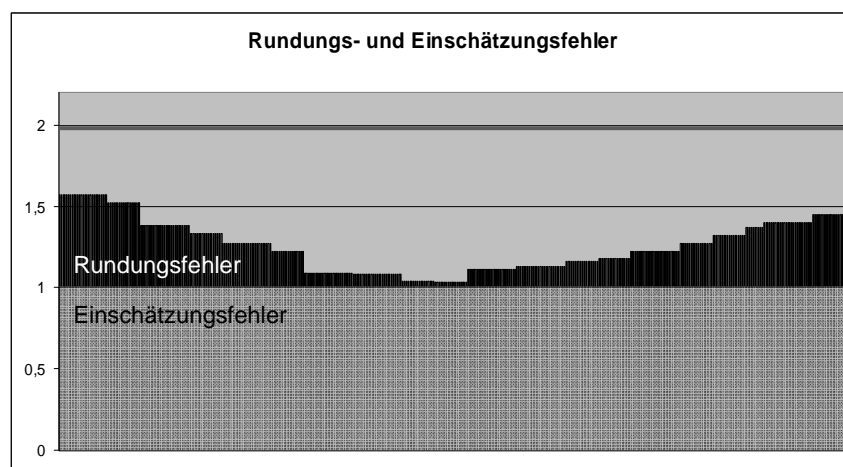


Abbildung 9-7 absoluter Rundungs- und Einschätzungsfehler

9.9 Anforderung A08

| Nr. | Anforderung |
|-----|---|
| A08 | Rigoreuse Begründung der Methode; umfassende und überprüfbare Dokumentation |

Es muss möglich sein, die Eigenschaften der Risikobeurteilungsmethode mit vernünftigen Argumenten, vergleichbar mit einem Safety Case, nachzuweisen. Von der UNIFE wird dazu gefordert, dass:

- „die Wahl der Parameter, Zwischenergebnisse und Endergebnisse umfassend dokumentiert sein sollen, insbesondere hinsichtlich Einheiten und Referenzen, sowie dass
- alle eingesetzten Hilfsmittel (tools) validiert werden müssen bzw. es möglich sein muss, das Ergebnisdokument zu überprüfen (z. B. durch manuelle Durchsicht)“ (aus dem Englischen nach /114/).

Diese Anforderung wird durch die vorliegende Arbeit erfüllt, die durch Argumentation die Eigenschaften von BP-Risk nachweist und dokumentiert. Es wird dadurch möglich, eine manuelle Durchsicht durchzuführen, um die Annahmen und Begründungen zu überprüfen.

9.10 Anforderung A09

| Nr. | Anforderung |
|-----|--|
| A09 | Ergebnisse und Sicherheitsziel haben gleiches Format |

Die Ergebnisse der Risikobewertung müssen laut ERA-Anforderung das gleiche Format (Einheit) wie das funktionale Sicherheitsziel haben. Wenn das funktionale Sicherheitsziel eine Ausfallrate (beispielsweise die Anzahl funktionaler Ausfälle pro Betriebsstunde) hat, dann muss folglich das Ergebnis der Risikobewertung auch in Form einer Ausfallrate ausgewiesen werden.

Das in BP-Risk implementierte Sicherheitsziel (RAC-TS) hat die Einheit ‚Funktionsversagen pro Betriebsstunde‘. Die Ergebnisse der Risikobewertung in BP-Risk haben die Einheit ‚tolerierbare Gefährdung (oder Funktionsversagen) pro Stunde‘. Da eine Funktionsversagenart auf betrieblicher Ebene auch als Gefährdung bezeichnet werden kann, können diese beiden Einheiten als identisch angesehen werden.

9.11 Anforderung A10

| Nr. | Anforderung |
|-----|---|
| A10 | Fähigkeit, verschiedene Parameter auszugleichen |

Die Methode sollte die Fähigkeit haben, die verschiedenen Parameter auszugleichen, z. B. Schadensausmaß und Häufigkeit, um das RAC-TS Kriterium für nicht-katastrophale Gefährdungen anwenden zu können. In den UNIFE Empfehlungen findet sich für diese Anforderung der Begriff „trade-off“ wieder: *„die Methode soll dazu fähig sein ein ‚trade-off‘ zwischen den verschiedenen Parametern durchzuführen“* (aus dem Englischen nach /114/).

Der Begriff ‚trade-off‘ beschreibt im Allgemeinen eine wechselseitige Abhängigkeit zweier Aspekte. Ein Trade-off liegt dann vor, wenn man eine Verbesserung oder Erlangung eines Aspektes nur unter Inkaufnahme der Verschlechterung oder des Verlustes des anderen Aspektes erreichen kann. In der Ökonomie beschreibt Trade-off z. B. die wechselseitige Abhängigkeit von Kosten und Qualität. Um eine hohe Qualität zu erlangen, muss man hohe Kosten in Kauf nehmen. Wenn man die Kosten senkt, sinkt auch die Qualität. Zwischen diesen beiden Eigenschaften besteht also ein Trade-off, über den man im konkreten Fall immer wieder neu entscheiden muss.

Die oben genannte Anforderung an Risikobeurteilungen meint mit Trade-off die wechselseitige Abhängigkeit der verschiedenen Risikoparameter. Trade-off bedeutet in diesem Fall eine plausible Abwägung oder Kompensation. Ziel dabei ist, die Risikoparameter so zu verändern bzw. eine Kombination zu finden, dass das Gesamtrisiko konstant bleibt.

Als Beispiel wird die oben eingeführte Beziehung des Risikos angenommen, also $Risiko = Häufigkeit * Gefahrenabwehr * Schaden$ oder $R = f * g * s$. Als tolerierbare Häufigkeit f_t wird angenommen $f_t = 10^{-9}/h$. In Anlehnung an RAC-TS hat der mit diesem Risiko verbundene Funktionsausfall ein glaubwürdiges, unmittelbares Potential (keine oder wenige Barrieren zwischen Gefährdung und Unfall) für einen katastrophalen Schaden. Im Rahmen einer Risikobeurteilung wird nun für eine Funktion die Häufigkeit $f_0 = 10^{-8}/h$ identifiziert. Angenommen, das Risiko bleibt konstant, dann können nun die Parameter s und g miteinander kombiniert werden. Die Häufigkeit f_0 besagt, dass das Funktionsversagen zehnmal häufiger auftreten darf im Vergleich zu f_t . Dies bedeutet, dass der Faktor 10 beim Schadensparameter oder beim Parameter Gefahrenabwehr ‚ausgeglichen‘ werden kann. So kann entweder eine niedrigere Schadensklasse (kritisch statt katastrophal) oder eine niedrigere Gefahrenabwehrstufe (mittelbar statt unmittelbar) gewählt werden (siehe Tabelle 9-7).

Tabelle 9-7 Trade-offs für Risikoparameter

| Risiko R | Häufigkeit f | Gefahrenabwehr g | Schaden s |
|----------|--------------|------------------|--------------|
| R_t | $10^{-9}/h$ | unmittelbar | katastrophal |
| R_0 | $10^{-8}/h$ | mittelbar | katastrophal |
| R_0 | $10^{-8}/h$ | unmittelbar | kritisch |

Dies setzt voraus, dass die verschiedenen Stufen innerhalb der Gefahrenabwehr und des Schadensausmaßes um den selben Faktor (hier: 10) auseinander liegen. Tabelle 9-7 macht deutlich, dass zur Erhöhung der zulässigen Häufigkeit eines Funktionsversagens entweder ein niedrigeres Schadenspotenzial oder eine geringere Gefahrenabwehr akzeptiert werden muss, um ein konstantes tolerierbares Risiko beizubehalten. Diese Fähigkeit hat jedoch den Vorteil, dass der Anwender entscheiden kann, an welchem Parameter er ‚drehen‘ muss, um dasselbe Ergebnis zu erhalten. Dies kann wirtschaftliche Vorteile mit sich bringen, da Maßnahmen zur Schadensbegrenzung andere Kosten haben können als Maßnahmen zur Gefahrenabwehr, so dass die kostengünstigere Variante gewählt werden kann, ohne dass dies Auswirkungen auf das tolerierbare Risiko hat.

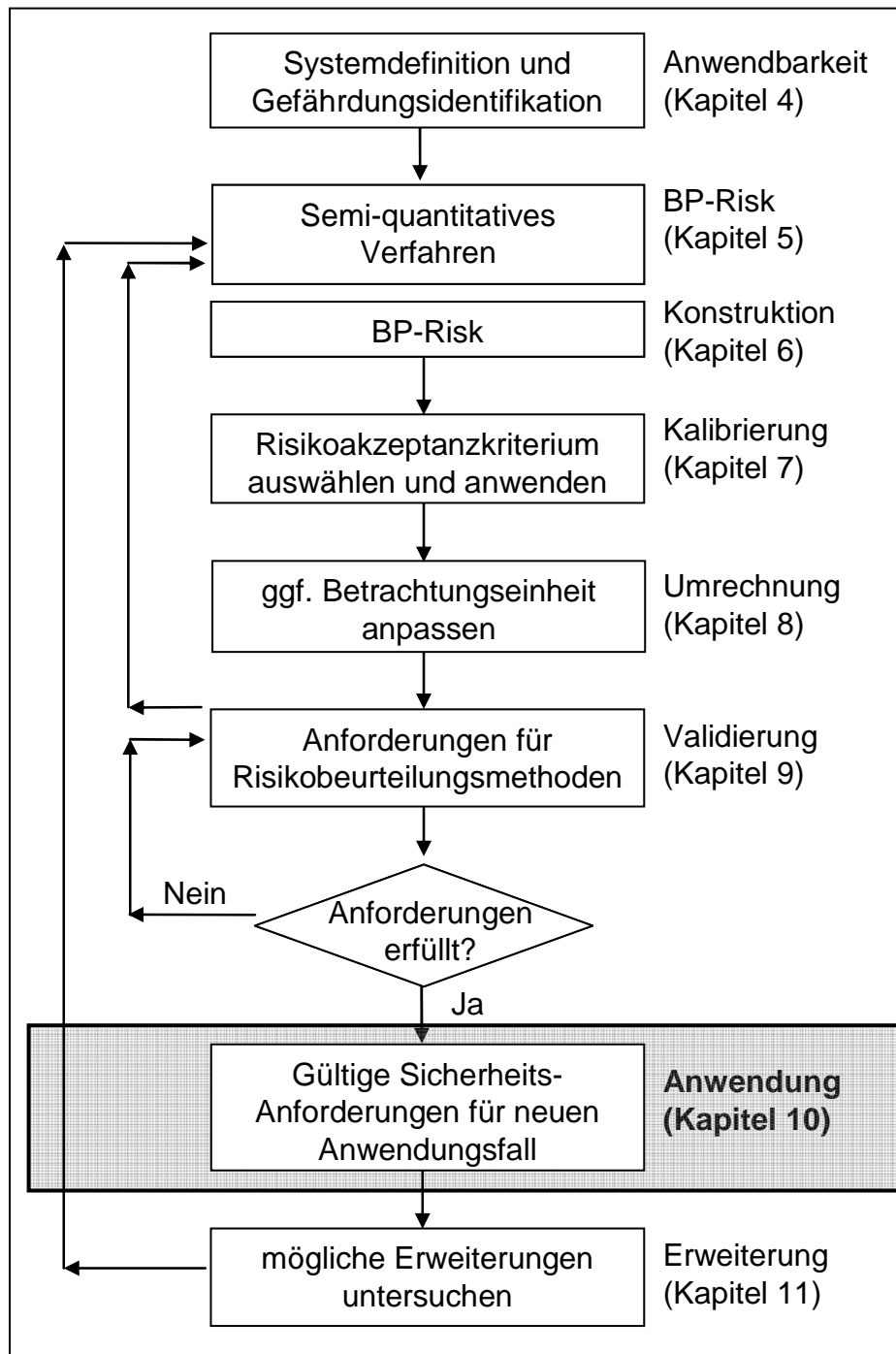
Nun lautet die Anforderung, dass eine optimale Methode zur Risikobeurteilung diese Trade-off Fähigkeit haben soll. Da BP-Risk auf einem generischen Risikomodell, der Form $R = f * g * s$ basiert, hat das obige Beispiel gezeigt, dass Trade-offs für solche Risikoformeln möglich sind. Somit wurde nachgewiesen, dass BP-Risk diese Eigenschaft auch besitzt. Durch die Subparameter von BP-Risk ist sogar ein Trade-off innerhalb der Parameter ‚Gefahrenabwehr‘ und ‚Schadenspotenzial‘ möglich.

9.12 Zusammenfassung

Um den Nachweis zu führen, dass es sich bei BP-Risk um eine nachvollziehbare und nach ingenieurwissenschaftlichen Prinzipien konstruierte Methode handelt, wurde in diesem Kapitel argumentativ gezeigt, dass BP-Risk die aufgestellten Anforderungen erfüllt.

- Es wurde gezeigt, dass RAC-TS als Risikoakzeptanzkriterium zu Grunde gelegt wurde und dies der europäischen Gesetzgebung entspricht.
- Eine Ermittlung des tolerierbaren Restrisikos ist nicht erforderlich, es ist per Konstruktion implementiert und wird nicht explizit ausgewiesen.
- Mensch und Technik sind aufgrund der Systemdefinition des Risikomodells, das dem Verfahren zugrunde liegt, mit einbezogen.
- Die unabhängige Bewertung der Systemfunktionen erfolgt aufgrund des Konstruktionsprinzips von BP-Risk; durch den mathematischen Ansatz können die einzelnen Einflussgrößen ebenfalls getrennt beurteilt werden.
- Qualitative Schadens- und Folgenanalyse sind ebenfalls aufgrund des Konstruktionsprinzips, insbesondere der Transformation und der Beschreibung der BP-Risk Tabellen, vorhanden; die Beschreibung der Tabelleneinträge der Teilparameter ist nachvollziehbar und prägnant.
- Alle relevanten Parameter der Risikoformel werden durch das BP-Risk-Risikomodell abgebildet oder implizit durch weiterführende Umrechnung berücksichtigt.
- Die Genauigkeitsanforderung wurde theoretisch und praktisch gezeigt; die festgestellten Abweichungen durch Einschätzungs- und Rundungsfehler bezogen auf die ermittelte THR liegen innerhalb einer Zehnerpotenz.
- Eine umfassende und überprüfbare Dokumentation liegt in Form dieser Arbeit vor und erlaubt die Überprüfung der Annahmen und Eigenschaften; die Forderung, dass die Information verfügbar ist, wie die Festlegung der Parameter zustande kam, kann somit erfüllt werden.
- Per Konstruktion hat das implementierte Sicherheitsziel (Risikoakzeptanzkriterium) die gleiche Einheit wie das Ergebnis der Risikobewertung.
- Aufgrund des zugrunde liegenden Risikomodells hat BP-Risk die Fähigkeit, die verschiedenen Risikoparameter auszugleichen.

Somit ist die argumentative und theoretische Validierung abgeschlossen. Im Folgenden wird nun BP-Risk für einen neuen Anwendungsfall eingesetzt, um dessen Tauglichkeit auch in der Praxis zu demonstrieren.



10 Neue Anwendung

Die Kosten für die Einführung von Sicherungstechnik (z. B. in Form von Signaltechnik) sind in der Regel sehr hoch. Dies ist bedingt durch beträchtliche Investitions- und Instandhaltungskosten. Somit ist die Erlössituation für Eisenbahninfrastrukturunternehmer auf Nebensrecken mit geringer Streckenauslastung ungünstig. Da eine technische Zugfolgesicherung auf Nebenbahnen nicht zwingend vorgeschrieben ist, kann der Zugleitbetrieb (ZLB) als kostengünstiges Betriebsverfahren auf Nebenbahnen eingesetzt werden. Die Reduzierung der Betriebskosten für den ZLB resultiert vor allem aus dem weitgehenden Verzicht auf Signaltechnik sowie der Zentralisierung der Betriebsführung in Verbindung mit der Reduzierung des erforderlichen Betriebspersonals auf den einzelnen Betriebsstellen. Als Konsequenz steht jedoch keine Technik zur Verfügung, die das menschliche Handeln kontrolliert. Innerhalb des Zugleitbetriebs hat der Mensch also eine hohe Sicherheitsverantwortung, so dass verstärkt nach technischen Lösungen gesucht wird, die die Sicherheit des ZLB noch unterhalb der ‚teuren‘ Signaltechnik verbessert.

Erste Ideen und Anwendungen von einfachen Einrichtungen zur Erhöhung der Sicherheit beim ZLB gab es bereits Anfang der 1980er Jahre. Verstärkt wurde in deren Entwicklung ab Ende der 1990er Jahre investiert. Diese Aktivitäten bildeten auch die Grundlage für Überlegungen im Zuge der Überarbeitung der VDV-Schrift 752, die heute eine technische Unterstützung für bestimmte Anwendungsfälle des ZLB fordert (siehe Anhang G: VDV-Schrift 752).

Die Akzeptanz technischer Sicherungssysteme für einfache betriebliche Verhältnisse ist laut EBA (/71/) aus der Ableitung von Sicherheitsanforderungen an die Technik mit Hilfe einer Risikobeurteilung möglich. Dies ist zurzeit noch ein Forschungsvorhaben, hat aber die Aussicht, dass bei erfolgreicher und akzeptierter Risikobeurteilung eine langfristige Sicherheit für Nebenstrecken gewährleistet werden kann. Da für einfache Technik bei einfachen Betriebsverhältnissen keine Gestaltungsnormen für technische Systeme (wie z. B. die EN 50129 für Signaltechnik) vorhanden sind, können somit keine anerkannten Regeln der Technik angewendet werden. Als Referenzsystem käme nur der Funkfahrbetrieb (FFB) in Frage, da ihm das ZLB-Prinzip zugrundeliegt, er jedoch auf einer sicherungstechnisch höherwertigen Ebene umgesetzt wird (/66/, Seite 452). Allerdings hat sich FFB in der Praxis nicht bewähren können, da er bislang nicht eingeführt wurde. Somit kann er laut ERA nicht als Referenzsystem⁶⁰ herangezogen werden. Im Folgenden wird somit eine explizite Risikoeinschätzung für das Betriebsverfahren Zugleitbetrieb anhand des neuen ERA-Prozesses und mit Hilfe von BP-Risk durchgeführt.

⁶⁰ Referenzsystem: bezeichnet ein System, das sich im Betrieb im Hinblick auf ein akzeptables Sicherheitsniveau bewährt hat und das als Vergleichssystem herangezogen werden kann, wenn ein System, das einer Bewertung unterzogen wird, auf die Vertretbarkeit seiner Risiken geprüft wird (/59/).

10.1 Zugleitbetrieb

Ein Betriebsverfahren ist ein „System betrieblicher Regeln und technischer Mittel zur Durchführung von Fahrten mit Eisenbahnfahrzeugen auf einer Eisenbahninfrastruktur“ (/95/). Der Zugleitbetrieb ist ein „Betriebsverfahren für Strecken mit einfachen Verhältnissen, bei dem die Zugfolge einer Strecke durch einen Zugleiter mittels fernmündlicher Meldungen geregelt wird“ (/95/). Strecken mit einfachen betrieblichen Verhältnissen zeichnen sich aus durch:

- „eine nur regionale Bedeutung,
- die Widmung als Nebenbahn,
- ein starres Betriebsprogramm,
- einen Zugfolgeabstand im Personenverkehr von einer Stunde und mehr,
- geringe Streckenhöchstgeschwindigkeiten, sowie
- kurze Streckenlängen in Verbindung mit nur wenigen Kreuzungsbahnhöfen sowie wenig Güterverkehr oder Rangierbetrieb“ (/107/, Seite 9).

Zwingende Voraussetzungen für den ZLB sind:

- „Nebenbahn mit Streckengeschwindigkeit ≤ 80 km/h (Forderung der EBO),
- eingleisige Strecke, und
- Vorhandensein einfacher betriebliche Verhältnisse gemessen an einem Bewertungsfaktor für die Streckenbelastung (VDV 752⁶¹)“ (/107/, Seite 21).

Die betrieblichen Regeln für dieses Verfahren sind in der DB Konzernrichtlinie 436 enthalten. Es gibt auch Vorgaben für den sogenannten Signalisierten Zugleitbetrieb (SZB) nach Richtlinie 437, die im Folgenden jedoch nicht betrachtet werden. Für die Nichtbundeseigenen Eisenbahnen ist das Betriebsverfahren Zugleitbetrieb Bestandteil der „Fahrdienstvorschrift für Nichtbundeseigene Eisenbahnen“ (FV-NE). Es gibt zum Teil unterschiedliche Begrifflichkeiten in den Vorschriften der DB und der NE-Bahnen. Im Folgenden wird versucht, möglichst allgemein verständliche Begriffe zu benutzen, so dass die Bedeutung und der Zweck klar werden. Das Zugleitverfahren wird nun kurz erklärt, wobei nur die wichtigsten Aspekte wiedergegeben werden (weitere Details befinden sich in den genannten Vorschriften und in der allgemeinen Fachliteratur, z. B. /95/ und /107/).

Die Strecken im Zugleitbetrieb werden als Zugleitstrecken bezeichnet, die im Regelfall an eine benachbarte Zugmeldestelle grenzen. In Einzelfällen grenzt sie an eine andere Zugleitstrecke. Bahnhöfe und Haltepunkte der Zugleitstrecke sind sogenannte Zuglaufstellen. Diese sind in der Regel nicht mit örtlichem Betriebspersonal besetzt, so dass im Rahmen der Systemdefinition von unbesetzten Zuglaufmeldestellen ausgegangen wird. Dort, wo es aufgrund der örtlichen Gegebenheiten erforderlich ist, können Zuglaufstellen durch einen örtlichen Bahnhofsfahrdienstleiter (nach KoRil 436) bzw. einen örtlichen Betriebsbediensteten (nach FV-NE) besetzt sein. Eine Besetzung durch örtliches Personal ist erforderlich, wenn z. B.

⁶¹ Siehe dazu auch Anhang G: VDV-Schrift 752.

- eine Schranke zu bedienen ist,
- der Fahrplan drei Züge gleichzeitig im Bahnhof vorsieht,
- hoher Rangieraufwand herrscht (nach /107/, Seite 29).

Für die Regelung der Zugfolge auf der gesamten Zugleitstrecke ist der Zugleiter (Zl) verantwortlich. Er regelt innerhalb der Zugleitstrecke die Zugfolge und die Zugreihenfolge, stimmt den Zugfahrten zu und erteilt die Erlaubnis zum Rangieren. Die erforderlichen Meldungen führt der Zl mit dem Zugführer (Zf)⁶² durch. Sie werden Zuglaufmeldungen genannt (siehe auch Abbildung 10-1). Wenn zusätzliche technische Sicherungseinrichtungen fehlen, basiert die Sicherheit des Zugverkehrs ausschließlich auf der ordnungsgemäßen Durchführung und Dokumentation dieser Meldungen.

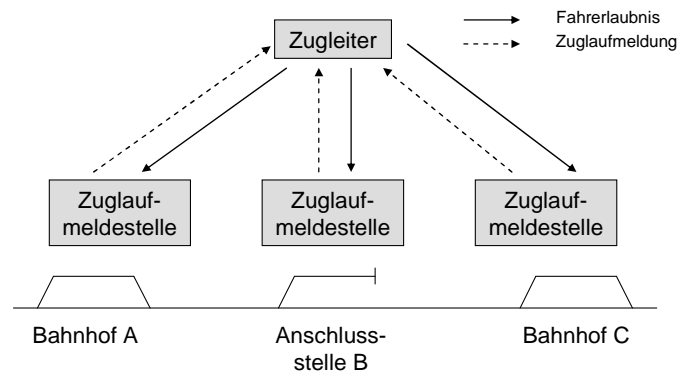


Abbildung 10-1 Grundprinzip des Zugleitbetriebs (nach /97/)

Die Stellen, an denen eine Zuglaufmeldung abzugeben ist, werden Zuglaufmeldestellen genannt (Anschlussstellen können auch Zuglaufmeldestellen sein). Die Zuglaufmeldungen werden auf unbesetzten Zuglaufmeldestellen zwischen dem Zl und dem Zf ausgetauscht. Bei Verwendung von Zugfunk werden die Zuglaufmeldungen fernmündlich durch den Tf übermittelt, hierbei sind feste Wortlaute vorgeschrieben.

Durch die zentrale Betriebsführung kann der Zl bestimmte Aufgaben eines Fahrdienstleiters im Zugmeldeverfahren nicht wahrnehmen, da der Zl nicht auf die Außenanlagen einwirken kann, z. B.:

- „die Fahrwegprüfung durch Hinsehen,
- das Einstellen und Sichern des Fahrweges,
- die Zustimmung zur Fahrt durch Fahrtstellung eines Signals sowie
- die Zugschlusserkennung und damit die Räumungsprüfung“ (/107/, Seite 21).

Um die fahrdienstlichen Aufgaben zu erfüllen, ist eine Einbindung des Zugpersonals zwingend erforderlich. Eine Vereinbarung der Zugreihenfolge zwischen zwei Betriebsstellen ist (innerhalb der Zugleitstrecke) nicht erforderlich, da der Zl für die gesamte Strecke verantwortlich ist. Die Zugfolge wird ausschließlich durch die Abgabe von Zuglaufmeldungen zwischen Zl und Zf geregelt.

⁶² Die Aufgaben des Zugführers können auch vom Triebfahrzeugführer (Tf) wahrgenommen werden.

10.1.1 Zuglaufmeldungen

Die Zuglaufmeldungen sind für die sichere Betriebsführung von zentraler Bedeutung. Sie sind das Instrument des Zugleiters, um Informationen über den Standort bzw. die Position der Züge und damit über die Belegung bzw. das Freisein von Gleis- und Streckenabschnitten zu erhalten und um Zugfahrten auf dieser Basis zuzulassen. Der Zf erfährt dadurch, ob und wie weit sein Zug fahren darf (nach /107/, Seite 31).

„Im Zugleitbetrieb gibt es folgende Zuglaufmeldungen:

- Fahrerlaubnis,
- Ankunfts meldung,
- Verlassensmeldung,
- Fahrwegsicherungsmeldung, und
- Abstellmeldung“ (/96/, Seite 44).

Die Fahrerlaubnis (Fe) wird nach den Angaben im Fahrplan oder schriftlichen Befehl angefordert. Es müssen alle Voraussetzungen für die Weiterfahrt des Zuges erfüllt sein, die vom Zugpersonal festzustellen sind. Diese können im Einzelfall sehr variieren, z. B. in Abhängigkeit davon, ob der Zug neu gebildet oder ob am Zug rangiert wurde.

Die Anforderung erfolgt durch eine Fahr anfrage des Zugführers, wobei die Fahrerlaubnis ab dem Standort des Zuges gilt. Als Ziel der Anfrage gilt die Zuglaufstelle, auf der die nächste Fahrerlaubnis eingeholt werden muss. Ansonsten gilt als Ziel der Endbahnhof des Zuges innerhalb der Zugleitstrecke oder die erste Zugmeldestelle nach Verlassen der Zugleitstrecke. Muss der Zug an der Trapeztafel (siehe Abbildung 10-2) der benannten Zuglaufmeldestelle anhalten, so wird dies durch den Fahrplan (Buchfahrplan siehe Kapitel 10.1.3) oder mittels Befehl dem Zf bekanntgegeben. Eine Fahrerlaubnis darf bis zu einer Zuglaufstelle nur erteilt werden, wenn der Abschnitt nicht durch einen anderen Zug beansprucht wird. Sie darf allerdings durch den ZI bis zu 10 Minuten vor der voraussichtlichen Abfahrt des Zuges gegeben werden.

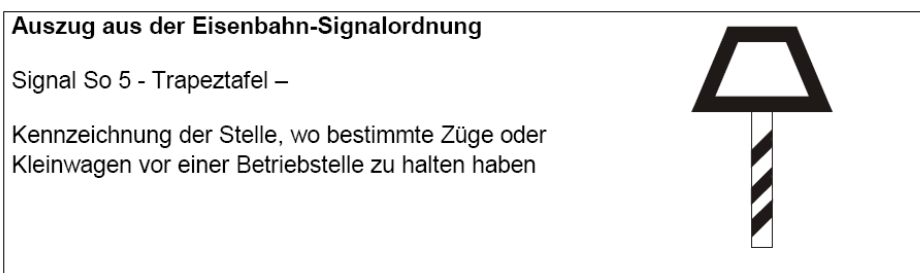


Abbildung 10-2 Trapeztafel (/57/)

Die Ankunfts meldung (Ak) wird durch den Zf an den ZI gegeben, wenn der Zug mit Schluss-signal an der Zugschlussstelle für die Einfahrt vorbeigefahren ist, bzw. die letzte Weiche des Einfahrweges geräumt hat. Die Zugvollständigkeit kann auf unbesetzten Betriebsstellen nur vom Zf festgestellt werden.

Die Verlassensmeldung (Ve) wird durch den Zf an den Zi auf unbesetzten Zuglaufmeldestellen gegeben. Sie darf erst erfolgen, wenn der Zug mit Schlusssignal an der Zugschlussstelle für die Ausfahrt bzw. an der Trapeztafel der Gegenrichtung vorbeigefahren ist und der Fahrweg für den nachfolgenden Zug eingestellt ist. Die Verlassensmeldung ist die einzige Zuglaufmeldung, die während der Fahrt abgegeben werden darf.

Die Fahrwegsicherungsmeldung (FsE) an den Zi wird vom Zf des ersten Zuges auf unbesetzten Zuglaufmeldestellen ohne Rückfallweichen gegeben, wenn das Zugpersonal des zuerst eingefahrenen Zuges den Fahrweg für den zweiten Zug einstellen muss (siehe auch Kapitel 10.1.2). Die Meldung erfolgt, wenn der Fahrweg für den zweiten Zug frei ist, die Weichen und Flankenschutzeinrichtungen sich in der richtigen Stellung befinden, gesichert sind und Rangierbewegungen auf den Hauptgleisen eingestellt wurden. Für den Entfall der Fahrwegsicherungsmeldung muss zusätzlich zu den Rückfallweichen auch noch Richtungsbetrieb⁶³ in den Bahnhofsgleisen vorhanden sein.

Rückfallweichen sind Weichen, die aufgefahren werden dürfen und die durch eine Rückstellmechanik anschließend wieder in die Ausgangslage laufen (nach /95/). Eine Rückfallweiche lässt sich während des Rangierens wie eine ortsgestellte Weiche mit Hilfe eines Hebelgewichtes umstellen. Zur Überwachung der korrekten Endlage der Rückfallweiche ist ein Überwachungssignal bzw. Deckungssignal vor der Weichenspitze aufgestellt (siehe Abbildung 10-3). In spitz befahrener Richtung muss der Tf die sichere Endlage der Weiche durch Beobachtung des Überwachungssignals prüfen und ggf. vor der Weiche anhalten.

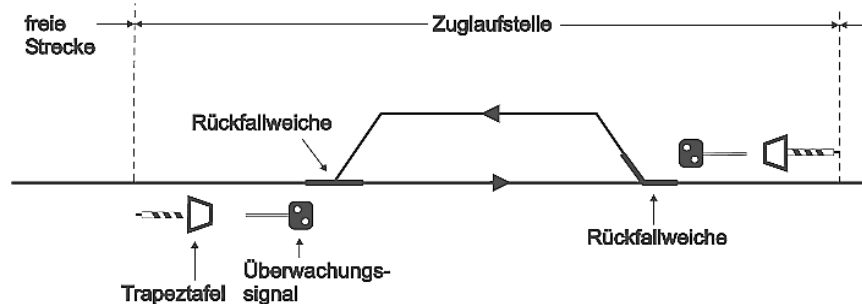


Abbildung 10-3 Zuglaufstelle (/118/)

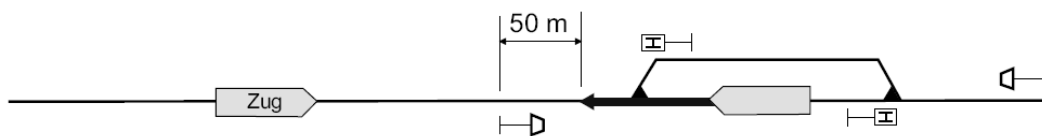
Die Abstellmeldung (As) an den Zi wird vom Zf auf unbesetzten Zuglaufstellen gegeben. Sie darf nur erfolgen, wenn die Rangierfahrt im Nebengleis abgestellt ist, in den Hauptgleisen keine Fahrzeuge zurückgelassen wurden und der Zugführerschlüssel sich in Verwahrung des Meldenden befindet. Der Abstellmeldung muss immer eine Ankunfts- oder eine Rangiererlaubnis vorausgegangen sein. Die Zuglaufmeldestelle ist damit frei für weitere Zugfahrten, so dass die Abstellmeldung, wie die Ankunfts- und Verlassensmeldung, einer Gleisfreimeldung entspricht.

⁶³ Richtungsbetrieb: ist hier in dem Sinne gemeint, dass die Bahnhofsgleise richtungsgebunden benutzt werden.

Auf unbesetzten Zuglaufstellen darf ohne Zustimmung des Zugleiters rangiert werden, wenn keine Zuglaufmeldung (ausgenommen eine Abstellmeldung) zu geben ist. Ansonsten darf nur mit Genehmigung des Zugleiters rangiert werden. Der ZI darf die Genehmigung nur erteilen, wenn er keinen Zug nach dieser Zuglaufstelle hat abfahren lassen oder wenn sichergestellt ist, dass ein abgefahrener Zug vor der Trapeztafel zum Halten kommt. Im letzteren Fall ist beim Rangieren ein Durchrutschweg von 50m hinter der Trapeztafel frei zu halten (siehe Abbildung 10-4). Über die Rangiertafel oder Einfahrweiche darf nur mit schriftlichem Befehl des Zugleiters rangiert werden. Die Rangiererlaubnis entspricht im funktionalen Sinne eigentlich einer Fahrerlaubnis.

Rangiergrenze

a) entgegen kommender Zug auf der Strecke



b) kein entgegen kommender Zug auf der Strecke

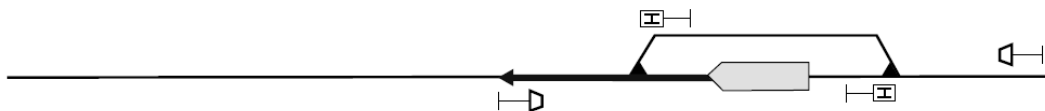


Abbildung 10-4 Rangieren im Zugleitbetrieb (/97/)

10.1.2 Fahrwegsicherung

Das Einstellen und Sichern des Fahrwegs in den Bahnhöfen ist in den Vorschriften geregelt und ist abhängig davon, ob der Bahnhof besetzt ist und ob Rückfallweichen vorhanden sind. Für verschlossene Weichen der Zugleitstrecke befindet sich in der Regel ein zentraler Zugführerschlüssel beim ZI, der nach Erfordernis an den Zf ausgehändigt wird (/107/, Seite 29).

In unbesetzten Bahnhöfen (Zuglaufstellen) ohne Rückfallweichen sind meist Handweichen vorhanden, die in Grundstellung verschlossen sind. Es gibt aber auch Bahnhöfe, in denen die Weichen von einer Hebelbank aus (durch das Zugpersonal) ferngestellt werden. Fährt ein Zug durch den Bahnhof, ohne dass eine Zugkreuzung stattfindet, ist ein Umstellen der Weichen nicht erforderlich.

Bei der Abwicklung von Zugkreuzungen ist der Zf des zuerst einfahrenden Zuges für die örtliche Fahrdienstleitung während der Kreuzung zuständig. Der erste Zug fährt ohne Halt an der Trapeztafel in den Bahnhof ein. Dessen Zf führt den Zugführerschlüssel mit. Zur Durchführung der Kreuzung sind dann zwei Verfahren möglich (siehe Abbildung 10-5 und Abbildung 10-6).

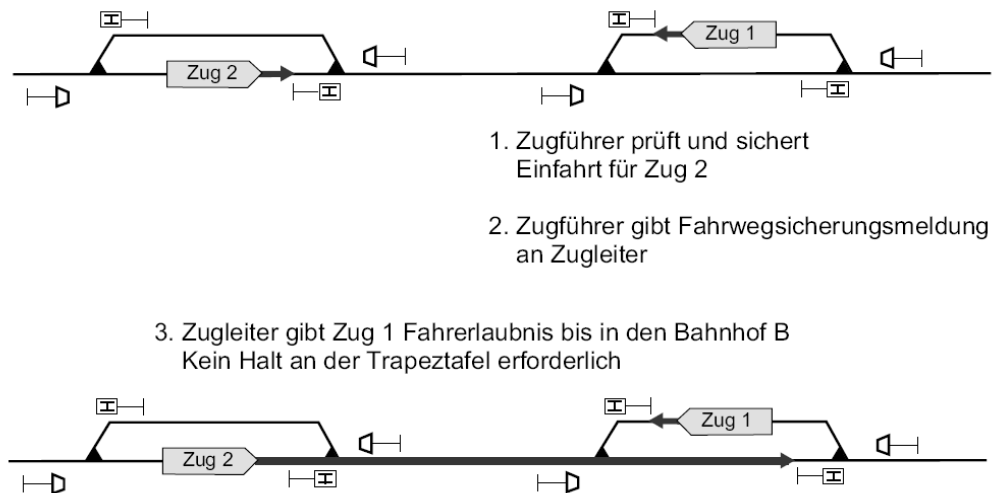


Abbildung 10-5 Kreuzung auf unbesetztem Bahnhof - Variante 1 (97/)

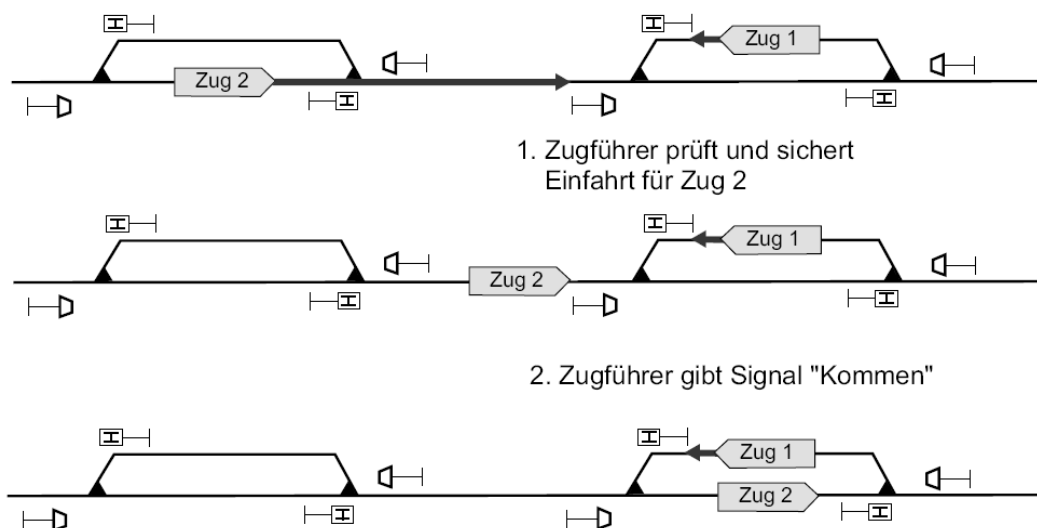


Abbildung 10-6 Kreuzung auf unbesetztem Bahnhof – Variante 2 (97/)

Hat der zweite Zug den Bahnhof verlassen, bringt das Zugpersonal des ersten Zuges die Weichen wieder in Grundstellung und verschließt diese. Dies ist Voraussetzung für die Weiterfahrt des ersten Zuges. Dieses Verfahren wird heute für planmäßig kreuzende Züge nur noch selten angewendet. Nachteil ist die lange Aufenthaltszeit des zuerst einfahrenden Zuges (nach /107/, Seite 30). Alternativen dazu bilden die Verwendung von Rückfallweichen oder elektrisch ortsgestellte Weichen (EOW), die jedoch bereits eine technische Lösung darstellen und deswegen im Rahmen der Risikobeurteilung vorerst nicht betrachtet werden. Die Funktionen „Fahrweg einstellen und Fahrweg sichern“ bleiben unabhängig von der Ausrüstung der Betriebsstelle erhalten.

Das Freisein der Hauptgleise der Zuglaufmeldestellen und der Streckenabschnitte wird durch den ZI mittels Zuglaufmeldungen festgestellt und dokumentiert. Der ZI führt vor dem Erteilen der Fahrerlaubnis eine Fahrwegprüfung durch. Die Gleise einer unbesetzten Zuglaufstelle gelten als frei, wenn

- eine Verlassensmeldung für diese Zuglaufstelle,
- eine Abstellmeldung für diese Zuglaufstelle,
- eine Ankunftsmeldung von einer weiter gelegenen Zuglaufstelle, oder
- die Rückmeldung von einem benachbarten Fahrdienstleiter oder ZI vorliegt. Dies ist im Meldebuch für den ZI bzw. Belegblatt für den ZI eingetragen.

Wenn ein Zug vollständig auf einer Betriebsstelle angekommen ist, kann daraus geschlossen werden, dass der zurückliegende Abschnitt frei ist. Die Ankunft mit Zugschluss auf dem Bahnhof wird dem ZI durch den Zf gemeldet. Aus der Ankunftsmeldung in einer Zuglaufstelle bzw. der Verlassensmeldung für eine Zuglaufstelle kann also auf das Freisein der zurückliegenden Streckenabschnitte oder Bahnhofsgleise geschlossen werden.

Es ist zu beachten, dass die FV-NE zur Flexibilisierung des Betriebsablaufes die Möglichkeit der ‚Vorsichtigen Einfahrt‘ (vE) gibt (/107/, Seite 38). Diese wird in übersichtlichen Bahnhöfen angewendet, wenn eine Fe bis in einen Bahnhof erteilt werden soll, der noch durch den vorausfahrenden Zug belegt ist. Für diesen vorausfahrenden Zug muss eine Ak in diesem Bahnhof vorliegen, die Fe für den nachfolgenden Streckenabschnitt erteilt und die Abfahrtszeit erreicht sein. Für den nachfolgenden Zug darf dann eine Fe bis in diesen Bahnhof erteilt werden, wenn er im Fahrplan, durch Eintrag im Fahrtbericht oder per Befehl durch das Zeichen ‚vE‘ den Auftrag hat, ab der Trapeztafel der Zuglaufstelle auf Sicht zu fahren. Die Fahrwegprüfung und ‚eigene‘ Gleisfreimeldung erfolgt ab der Trapeztafel also durch den Zf. Es wird davon ausgegangen, dass der Bahnhof aufgrund der oben genannten Vorbedingungen frei sein müsste, bis der Zug, für den die vorsichtige Einfahrt vorgeschrieben ist, diesen erreicht hat. Das ist zum Zeitpunkt des Erteilens der Fe jedoch noch nicht durch eine Ve oder eine Ak in einem weiter entfernt liegenden Bahnhof dokumentiert. Da dieser Fall dem eigentlichen Prinzip des ZLB (zentralisierte Fahrdienstleitung) widerspricht, wird dieser in der folgenden Risikobeurteilung nicht berücksichtigt.

Ausgenommen von der Fahrwegsicherung im ZLB ist die Sicherung von Bahnübergängen. Dazu gibt es eigene Sicherheitsbetrachtungen. Die EBO §11(7) legt fest, dass die Sicherung beispielsweise bei schwachem oder mäßigem Straßenverkehr (d. h. 100 – 2500 Kfz pro Tag) durch die Übersicht auf die Bahnstrecke in Verbindung mit hörbaren Signalen des Eisenbahnfahrzeugs erfolgen muss. Bei fehlender Übersicht erfolgt die Sicherung (mit besonderer Genehmigung) durch hörbare Signale des Eisenbahnfahrzeugs, wenn die Geschwindigkeit des Eisenbahnfahrzeugs am BÜ höchstens 20km/h – an BÜs von Feld- und Waldwegen höchstens 60 km/h beträgt.

10.1.3 Betriebliche Unterlagen

Im Buchfahrplan wird für die jeweilige Zugfahrt vorgeschrieben, auf welchen Stellen Zuglaufmeldungen abzugeben sind. Der Buchfahrplan ist eine Fahrplanunterlage für den Tf, die dieser aufgeschlagen auf seinem Führerraumtisch vor sich liegen haben muss. Aus dem Buchfahrplan für den ZLB sind u. a. folgende Angaben ersichtlich (siehe Abbildung 10-7):

- abzugebende Zuglaufmeldungen und durch wen dies erfolgt,
- Stellen der Geschwindigkeitswechsel,
- zulässige Geschwindigkeiten der freien Strecke und in den Bahnhöfen,
- Züge, mit denen gekreuzt wird,
- Züge, die überholen oder überholt werden,
- Züge, die an der Trapeztafel anzuhalten haben, sowie
- das Gleis, in welches in Bahnhöfen eingefahren wird.

| 1 | 2 | 3a | 3b | 4 | 5 | 6 | 7 | 8 | 9 |
|-----------------------------|------|-----------------|------------|-----------------------------|---------|---------|----------------|----------------------------------|--------------------------------|
| Zulässige Geschwindigkeiten | | Betriebsstellen | Lage in km | An der Trapeztafel hält Zug | Ankunft | Abfahrt | Kreuzt mit Zug | Überholt wird überholt durch Zug | Zuglaufmeldungen durch Art |
| ab km | km/h | | | | | | | | |
| 1,0 | 40 | A-Stadt | 0,0 | | | | | | Zf Fe |
| 11,1 | 60 | | | | | | | | |
| 12,2 | 40 | B-Stadt | 11,7 | | 10.04 | 10.05 | | | |
| 19,9 | 60 | | | | | | | | |
| 20,7 | 40 | C-Stadt | 20,2 | | 10.15 | 10.21 | 3366 | | Zf Ak+Fe Zf f 3366 Ak+Fe |

Abbildung 10-7 Buchfahrplan (fiktiver Ausschnitt nach /107/, Seite 50)

Die Zuglaufmeldungen werden durch den ZI in ein Zugmeldebuch (bzw. Meldebuch oder Belegblatt für den ZI bei den NE-Bahnen⁶⁴) eingetragen. Der ZI erfasst den Belegungszustand der Zuglaufstellen und Streckenabschnitte durch eine grüne (hier: hellgraue Schlangenlinien) Frei- oder eine rote (hier: dunkelgraue Pfeile) Belegtlinie (siehe Abbildung 10-8). Auf der Basis der vorgenommenen Eintragungen entscheidet der ZI über das Zulassen von Zugfahrten (Erteilung der Fahrerlaubnis). Aufgrund der beim ZLB fehlenden signaltechnischen Sicherungseinrichtungen ist somit nur anhand des Zugmeldebuches der Besetzt- bzw. Freistatus der Streckenabschnitte und Betriebsstellen feststellbar.

⁶⁴ Das Meldebuch für den Zugleiter ist ähnlich dem Zugmeldebuch für den ZLB nach Ko-Ril 436 aufgebaut. Das Belegblatt enthält jedoch eine grafische Darstellung der Streckenbelegung mittels Zeit-Weg-Linien.

| Tag | | Zuglaufmeldungen | | | | | | | | | | | Ver- merke | | | | |
|-----------|------|------------------|--------------------|----|------------------------------|------|---|-----|----|----|---------|------------------------------|---------------|---|----|---|--|
| 1 | 2 | 7a | 8a | | 9a | | | 10a | | 7b | 8b | | 9b | | 11 | | |
| Zugnummer | | Strecke | Adorf unbesetzt | | | | | | | | Strecke | Bdorf unbesetzt | | | | | |
| → | | | Ak | | Sonstige Zug- laufmeldung | | | Fe | | Ak | | Sonstige Zug- laufmeldung | | | | | |
| | ← | | Fe | | Art | Zeit | | Ak | | Fe | | Art | Zeit | | | | |
| | | | U | M | | U | M | U | M | | | | U | M | U | M | |
| Übertrag | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | 3881 | | 14 | 27 | | | | 14 | 28 | | 14 | 40 | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |

Abbildung 10-8 Zugmeldebuch (fiktiver Ausschnitt nach /107/, Seite 42)

Das Zugmeldebuch wird grundsätzlich für die gesamte Zugleitstrecke geführt und umfasst alle Zuglaufstellen sowie die benachbarten Betriebsstellen. Es werden hier alle Meldungen dokumentiert, die vom ZI abgegeben oder entgegengenommen werden. Das betrifft nicht nur die Zuglaufmeldungen, sondern auch die Zugmeldungen zum benachbarten Fahrdienstleiter. Damit hat der ZI einen Gesamtüberblick über seine Strecke.

Parallel dazu werden die abgegebenen Zuglaufmeldungen bei jedem Mitarbeiter, der Gespräche mit dem ZI führt, ebenfalls schriftlich dokumentiert. Somit ist eine Plausibilitätsprüfung der Eintragungen möglich. Die Zuglaufmeldungen werden durch den Zf in ein Fernsprechbuch (bzw. Meldebuch für Zuglaufmeldungen nach FV-NE) eingetragen (siehe Abbildung 10-9). Es gibt noch weitere Dokumente wie der Fahrtbericht nach VDV-Schrift 752 und auch Befehlsvordrucke für z. B. Fahren auf Sicht, Vorbeifahrt an haltzeigenden Hauptsignalen, Sperren von Gleisen usw., die hier nicht detaillierter vorgestellt werden (siehe dazu /107/, Seite 45ff).

| 1 | 2 | 3 | 4 | | | 5 | 6 | 7 | 8 | | | 10 |
|---------------------------|---------------------------|----------------------|---------------|----------|---------|---|----------------------------------|---------------------------------|---------------------------------|-------|--|--------------------------------|
| Tag Zuglauf- stelle | Zug- num- mer Rf | Ankunfts- meldung | Fahrerlaubnis | | | Fahrweg- sicherungs- meldung Gleis | Verlas- sens- mel- dung | Ran- gierer- laub- nis | Abstell- meldung in Gleis | | | Name des Zuglei- ters |
| | | U M | U M | bis..... | Nr | U M | U M | U M | Nr | U M | | |
| | | | 23.09.05 | | | | | | | | | |
| A-Stadt | 3701 | | 18 | 17 | C-Stadt | | | | | | | |
| C-Stadt | 3701 | 18 | 31 | 18 | 32 | G-Stadt | | | | | | |
| G-Stadt | 3701 | 18 | 51 | 18 | 52 | L-Stadt | | | | | | |
| L-Stadt | 3701 | 19 | 03 | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

Abbildung 10-9 Fernsprechbuch (fiktiver Ausschnitt nach /107/, Seite 48)

10.2 ERA Prozess

Der ERA Prozess im Rahmen der ersten Reihe der CSM muss für die durchzuführende Risikobeurteilung nicht zwingend angewendet werden, da es sich um keine signifikante Änderung des Eisenbahnsystems handelt. Der Zugleitbetrieb ist seit 1967 Bestandteil der EBO und damit anerkannte Regel der Technik. Gegebenenfalls würde die Einführung einer einfachen technischen Unterstützung eine signifikante Änderung darstellen. Im Folgenden wird daher die Systematik des ERA-Prozesses für eine generische Risikobeurteilung des ZLB befolgt, da er den aktuellsten Stand für Risikobeurteilungen darstellt. Der Prozess beschreibt dafür die folgenden Schritte (siehe auch Abbildung 2-2):

- Systemdefinition,
- Gefährdungsidentifikation (und Gefährdungsklassifikation),
- Risikoanalyse, und
- Risikobewertung.

Im vorliegenden Fall wird die Risikoanalyse mit Hilfe einer expliziten Risikoeinschätzung durchgeführt, in dem BP-Risk als Methode zur Anwendung kommt (siehe Abbildung 6-1). Da BP-Risk auf die Funktionsliste aus Anhang E: Funktionsliste eingestellt ist, erfolgt die Risikobeurteilung anhand der vorgegebenen Funktionen, um die korrekte Anwendungsebene für BP-Risk zu gewährleisten. Zusätzlich soll damit sichergestellt werden, dass die durch die Funktionsliste ermittelten Gefährdungen mit BP-Risk bewertet werden dürfen. Im Folgenden werden die einzelnen Prozessschritte detailliert beschrieben.

10.2.1 Systemdefinition

Nach der vorausgegangen, allgemeinen Beschreibung des Betriebsverfahrens Zugleitbetrieb erfolgt im ersten Schritt der Risikobeurteilung die Systemdefinition. Dabei gelten für das vorliegende Anwendungsbeispiel zusammenfassend folgende Annahmen (auch nach /37/):

- Nebenbahn mit einfachen betrieblichen Verhältnissen,
- eingleisige Strecke mit Personenverkehr,
- Güterverkehr und Rangierbetrieb werden nicht betrachtet,
- Streckenhöchstgeschwindigkeit beträgt 80 km/h,
- Zugfolgeabstand von einer Stunde (und mehr),
- Zuglaufmeldestellen sind unbesetzt,
- Zugleitstrecke grenzt an benachbarte Zugmeldestelle,
- Sicherung der Zugfolge erfolgt allein durch mündliches Zuglaufmeldeverfahren,
- keine Sicherungstechnik⁶⁵ vorhanden,
- keine Sicherheitsbetrachtung für Bahnübergänge.

⁶⁵ z.B. Ein- und Ausfahrtsignale, Signalabhängigkeit von Weichen, Gleisfreimeldung, Streckenblock, Zugbeeinflussung.

Zugleitstrecken mit Personenverkehr sind in der Regel mit Zugfunk und Rückfallweichen (als Standardausrüstung) ausgestattet. Da diese Einrichtungen jedoch bereits technische Lösungen darstellen, werden im Rahmen der Systemdefinition die daraus resultierenden (i. d. R. vereinfachenden) betrieblichen Abläufe, z. B. für Zuglaufmeldungen (siehe /107/, Seite 32) und Fahrwegsicherung (siehe /107/, Seite 30) vorerst nicht berücksichtigt.

Im Rahmen der Systemdefinition wird nun festgelegt, welche Funktionen aus der Funktionsliste (siehe Anhang E: Funktionsliste) für ZLB relevant sind. Es wird dabei davon ausgegangen, dass die Funktionen des Betriebsverfahrens ZLB sich aus Fahrzeug- und Streckenfunktionen zusammensetzen, denn laut oben genannter Definition besteht ein Betriebsverfahren aus betrieblichen Regeln und technischen Mitteln, um Fahrten mit Eisenbahnfahrzeugen auf einer Eisenbahninfrastruktur durchzuführen.

Die generische Risikobeurteilung wird durchgeführt für eine einfache technische Unterstützung, um die Sicherheit des ZLB zu verbessern. Dabei ist zu beachten, dass die einzusetzende Technik den Menschen lediglich überwachen soll, d. h. der Mensch darf sich nicht auf die Technik verlassen. Die menschlichen Handlungen, wie sie beim ZLB durch Regeln beschrieben sind, sollen vorerst erhalten bleiben. Nur die menschlichen Fehlhandlungen sollen aufgedeckt und durch eine Sicherungstechnik verhindert werden. Für die Bewertung im Rahmen der Risikobeurteilung wird (wie oben bei den Annahmen formuliert) erst einmal von den Basisfunktionen ausgegangen, so wie sie ohne Sicherungstechnik ablaufen würden.

Es geht hier also insbesondere um Funktionen, die die Sicherung der Zugfahrten betreffen. Diese Funktionen befinden sich in der Funktionsliste unter den Kategorien K und L wieder. Die anderen Kategorien sind im Rahmen eines Betriebsverfahrens nicht relevant, da sie zur Durchführung und Regelung von Zugfahrten nicht eingesetzt werden. Die K- und L-Funktionen sind im Anhang (siehe Anhang H: Funktionen ZLB) wiedergegeben, wobei sowohl die Relevanz für die Bewertung des Betriebsverfahrens und die nötige Interpretation der Funktionen für den ZLB als Kommentar hinzugefügt wurden. Zusammenfassend können folgende Funktionen für den ZLB konkretisiert werden (siehe Tabelle 10-1).

Tabelle 10-1 Betriebliche Funktionen im ZLB

| Code | Funktion aus Funktionsliste | Nr. | Betriebliche Funktion (ZLB) |
|-------|---|-----|--|
| KC | Fahrzeugidentifikation ermöglichen | 1 | korrekte Zugnummer angeben |
| KD | Betriebl. Datenübertragung ermöglichen | 2 | Weg- und Geschwindigkeitsinformationen |
| KE/KF | Zugsicherung- und steuerung ermöglichen | 3 | Fahrgrenzen und Geschwindigkeit überwachen |
| LBD | Zugbeeinflussung bereitstellen | | |
| KG | korrekte Fahrwegwahl gewährleisten | 4 | Fahrweg richtig einstellen |
| LBB | Gleisfreimeldung bereitstellen | 5 | Fahrwegprüfung und Gleisfreimeldung |
| LBC | Ortung bereitstellen | 6 | Streckenbeobachtung und Ortungsmeldung |
| LBF | Bewegliche Fahrwegelemente sichern | 7 | Fahrweg sichern |
| LBH | korrektes Fahrsignal anzeigen | 8 | Zustimmung zur Fahrt erteilen |

Auf Grundlage der betrieblichen Funktionen im ZLB werden im Folgenden die möglichen Gefährdungen aus dem Funktionsversagen ermittelt (kreative Phase).

10.2.2 Gefährdungsidentifikation

Die empirische Phase der Gefährdungsidentifikation betrachtet die Erfahrungen aus der Praxis, die gezeigt haben, dass ein Großteil der gefährlichen Ereignisse im Zugleitbetrieb folgende Ursachen haben:

- Abfahren ohne Fahrerlaubnis, und
- Erteilen einer Fahrerlaubnis, ohne dass die Voraussetzungen dafür erfüllt sind.

Abbildung 10-10 zeigt dazu eine Statistik des EBA über die Anteile der einzelnen Fehlhandlungen bei Gefährdungen im Zugleitbetrieb.

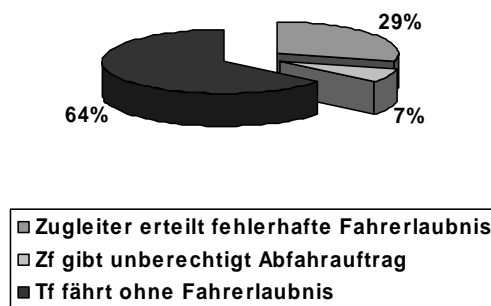


Abbildung 10-10 Ursachen der Gefährdungen im Zugleitbetrieb (nach /71/)

Es wird in /108/ (Seite 39) angemerkt, dass Fehler bei der Kommunikation sich in nahezu allen Fällen auf Fehlhandlungen des betreffenden Personenkreises zurückführen lassen, da im Regelwerk zum ZLB eindeutige Vorgaben hinsichtlich der Verständigung vorhanden sind. Somit verbleiben als Grundursachen (bei unbesetzten Zuglaufstellen) die Fehlhandlungen entweder des ZI oder des Zf.

Diese menschlichen Fehlhandlungen haben jedoch nicht nur Auswirkungen bezüglich der Erteilung einer Fahrerlaubnis, sondern auch hinsichtlich der Einstellung und Sicherung des Fahrwegs, die in /108/ nicht explizit als Gefährdung genannt werden.

Daher folgt im Rahmen der Risikobeurteilung auf Grundlage der aufgestellten Funktionen für den ZLB die kreative Phase der Gefährdungsidentifikation. Dazu wird für eine grobe Abschätzung aus der Liste der Systemfunktionen durch Negation eine Liste der Systemgefährdungen abgeleitet. Im Rahmen einer möglichen Ursachenanalyse kann dieses Ergebnis durch eine Schnittstellen-FMEA abgesichert werden. Negation bedeutet hier, dass überlegt wird, wie die Funktion versagen kann. Dabei kann es unter Umständen mehrere Versagensarten bei einer Funktion geben. Zu beachten ist außerdem, dass manche Ausfallarten im betrieblichen Kontext keinen Sinn ergeben. Darum wird in Tabelle 10-2 sowohl die Negation der Funktion genannt als auch die daraus hergeleitete betriebliche Gefährdung auf Basis der betrieblichen Funktionen des ZLB.

Tabelle 10-2 Gefährdungsliste durch Negation der Systemfunktionen

| Nr. | Funktion | Negation | Betriebl. Gefährdung |
|-----|---|--|--|
| 1 | Fahrzeugidentifikation ermöglichen (korrekte Zugnummer angeben) | Fahrzeugidentifikation nicht ermöglicht oder falsch durchgeführt | Falsche Zugnummer angegeben (betrifft Zuglaufmeldung) |
| 2 | Betriebl. Datenübertragung ermöglichen (Weg- und Geschwindigkeitsinfos bereitstellen) | Betriebl. Datenübertragung nicht ermöglicht oder verfälscht | Keine/falsche Weg- oder Geschwindigkeitsinfos bereitgestellt |
| 3 | Zugsicherung (Zugbeeinflussung) ermöglichen | Zugsicherung nicht ermöglicht | Fahrweggrenzen und zulässige Geschwindigkeit nicht oder falsch überwacht |
| 4 | Korrekte Fahrwegwahl gewährleisten (Fahrweg richtig einstellen) | Korrekte Fahrwegwahl nicht gewährleistet | Fahrweg nicht oder falsch eingestellt |
| 5 | Gleisfreimeldung bereitstellen (Fahrwegprüfung und Gleisfreimeldung) | Gleisfreimeldung nicht oder falsch bereitgestellt | Gleis fälschlicherweise freigemeldet (betrifft Zuglaufmeldung) |
| 6 | Ortung bereitstellen (Streckenbeobachtung und Ortungsmeldung) | Ortung nicht oder falsch bereitgestellt | Falsche Ortungsmeldung gegeben (betrifft Zuglaufmeldung) |
| 7 | Bewegliche Fahrwegelemente sichern (Fahrweg sichern) | Bewegl. Fahrwegelemente nicht oder falsch gesichert | Fahrweg nicht oder fehlerhaft gesichert |
| 8 | Korrektes Fahrsignal anzeigen (Zustimmung zur Fahrt erteilen) | Fahrsignal nicht korrekt angezeigt | Zustimmung zur Fahrt fälschlicherweise erteilt |

Die Funktionen 1, 5 und 6 übermitteln Informationen vom Zf zum Zi. Die Identifizierung des Fahrzeugs erfolgt durch die Nennung der Zugnummer bei jeder Zuglaufmeldung. Die Gleisfreimeldung und die Ortung erfolgen durch die eigentliche Beobachtung der Strecke und der Prüfung des Fahrwegs sowie durch die Abgabe einer Zuglaufmeldung (z. B. Ankunfts- oder Verlassensmeldung). Die Negation der Funktionen 1, 5 und 6 führen zu einer falschen oder verfälschten Zuglaufmeldung und werden deswegen zu einer Gefährdung zusammengefasst. Die Aufteilung der resultierenden Gefährdungsrate auf die ursprünglichen Funktionen bzw. auf konkrete Subsysteme (sobald die technische Realisierung bekannt ist) muss dann im Rahmen der Ursachenanalyse erfolgen.

Da im ZLB die betrieblichen Informationen in Form von Weg- oder Geschwindigkeitsinformationen auf sehr unterschiedliche Art und Weise übertragen werden, kommen Aspekte der Funktion 2 in anderen Funktionen vor und können somit Teil der Gefährdung sein. Beispielsweise könnten durch falsche Angaben im Buchfahrplan (z. B. falsche Kilometerangaben) falsche Zuglaufmeldungen abgegeben werden. Auch könnte durch eine falsche Geschwindigkeitsangabe die zulässige Geschwindigkeit nicht korrekt überwacht werden. Allerdings sind falsche Angaben im Buchfahrplan oder falsche Signaltafeln an der Strecke eher unwahrscheinlich, da diese Informationen nur einmal aufgestellt und ständig durch die betriebliche Nutzung überprüft werden.

Betriebliche Informationen werden jedoch auch über Zuglaufmeldungen oder schriftliche Befehle übermittelt, bei denen ein Übertragungsfehler schon eher vorkommen kann. Die Art und Weise, wie die betrieblichen Informationen übertragen werden, ist abhängig von der

technischen Realisierung. Funktional gesehen wären Fahrplan oder Signale überflüssig, wenn alle Informationen nur über fernmündliche Meldungen oder Signaltechnik abgewickelt würden. Deswegen wird der Aspekt der falschen betrieblichen Datenübertragung (Funktion 2) vorerst der Gefährdung ‚falsche/verfälschte Zuglaufmeldung gegeben‘ (Gefährdung G2) zugeordnet (siehe Tabelle 10-2), da die betriebliche Kommunikation im ZLB hauptsächlich über die Zuglaufmeldungen durchgeführt wird.

Auch hier muss im Verlauf einer anschließenden Ursachenanalyse die technische Realisierung berücksichtigt werden und ggf. die Gefährdungsrate auf mehrere Funktionen aufgeteilt werden.

Die Negation der Funktion Zugsicherung wird in zwei separaten betrieblichen Gefährdungen bewertet, nämlich Geschwindigkeit überwachen und Fahrgrenzen überwachen, da das Funktionsversagen möglicherweise zu verschiedenen betrieblichen Folgen führen kann.

Die Gefährdungen G1 und G2 müssen jeweils für zwei getrennte Szenarien bewertet werden, die abhängig von der Regelung der Zugkreuzungen sind (siehe Kapitel 10.1.2). Szenario a) betrachtet die jeweilige Zuglaufmeldung und Szenario b) die Regelung der Zugkreuzung durch das Signal „Kommen“. Für Gefährdung G5 müssen auch zwei Szenarien unterschieden werden, nämlich das Einstellen des Fahrwegs für einen anderen Zug (Szenario a) und das Herstellen der Grundstellung zur eigenen Weiterfahrt (Szenario b). Tabelle 10-3 fasst die resultierenden betrieblichen Gefährdungen des ZLB zusammen.

Tabelle 10-3 Betriebliche Gefährdungen des ZLB

| Nr. | Fkt. | Gefährdung | Beteiligte | |
|-----------|----------|--|------------|----------|
| G1 | a | Zustimmung zur Fahrt fälschlicherweise erteilt | Zl (Fdl) | Zf (Tf) |
| | b | | Zf (Tf) | |
| G2 | a | Falsche/verfälschte Zuglaufmeldung gegeben | Zf (Tf) | Zl |
| | b | | | |
| G3 | 3 | Fahrgrenzen nicht/fehlerhaft überwacht | Tf | Fahrzeug |
| G4 | 3 | Geschwindigkeit nicht/fehlerhaft überwacht | | |
| G5 | a | Fahrweg nicht/fehlerhaft eingestellt | Zf (Tf) | Fahrweg |
| | b | | | |
| G6 | 7 | Fahrweg nicht/fehlerhaft gesichert | | |

Eine Gefährdungsklassifikation, wie sie der ERA-Prozess fordert, wird an dieser Stelle nicht durchgeführt, da nur eine geringe Anzahl Gefährdungen betrachtet werden und davon auszugehen ist, dass diese bereits die signifikanten Gefährdungen darstellen.

10.2.3 Risikoanalyse

Nach erfolgter Gefährdungsidentifikation, besteht die explizite Risikoeinschätzung im ERA-Prozess aus den folgenden Schritten:

- Ermittlung von Szenarien und damit zusammenhängende Sicherheitsmaßnahmen,
- Entscheidung, ob die Risiken qualitativ oder quantitativ beurteilt werden,
- bei einer quantitativen Bewertung:
Abschätzung der Häufigkeit und der Schwere sowie des resultierenden Risikos.

BP-Risk ist eine semi-quantitative Methode, die hier den Grundsätzen einer quantitativen Beurteilung folgt (siehe Abbildung 10-11). Die Risikoanalyse mit Hilfe von BP-Risk beinhaltet eine vereinfachte Folgen- und Schadensanalyse sowie einer anschließende Risikobewertung (im ERA-Prozess ist dies ein eigener Schritt, siehe Kapitel 10.2.4).

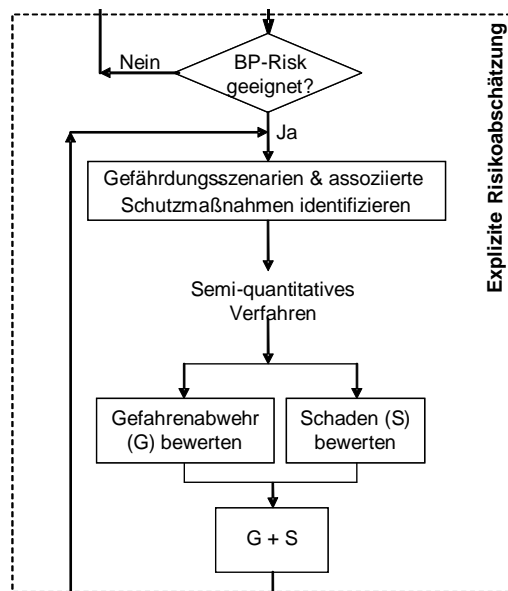


Abbildung 10-11 Explizite Risikoeinschätzung mit BP-Risk

Angewandt auf eine Gefährdung befasst sich die Folgenanalyse mit der Frage „Was passiert, wenn die Gefährdung eingetreten ist?“ Die Folgenanalyse dient der Identifizierung und Erfassung von wahrscheinlichen Konsequenzen, die sich aus einer Gefährdung ergeben können. So gesehen zählen alle Ereignisse, die nach Eintritt einer Gefährdung passieren, zu den möglichen Folgen. Ein Teil der Folgenanalyse wurde bereits durch die Zusammenfassung einiger Funktionsversagen im Rahmen der Gefährdungsidentifikation durchgeführt. Die Notwendigkeit einer Folgenanalyse für eine realistische Beurteilung des Risikos ergibt sich aus der Tatsache, dass längst nicht alle Gefährdungen zu Unfällen oder gar Katastrophen führen, sondern dass ein großer Teil dieser Situationen schadensfrei oder mit geringen Schäden endet. Bei der Folgenanalyse geht es vor allem um die Identifizierung verschiedener Schutzmaßnahmen, die die potenzielle Eskalation einer Gefährdung verhindern sollen. Dazu zählen im Rahmen von BP-Risk die standardisierten Risikoreduktionsfaktoren des Parameters G (Gefahrenabwehr).

Die Folgenanalyse dient der Vorhersage einer Reihe von Zwischen- und Unfällen, die sich nach Eintritt einer Gefährdung aus verschiedenen Kombinationen von Erfolg und Versagen der Schutzmechanismen ergeben. Die meisten Unfälle resultieren in einem Schaden, der abhängig von der Energie, dem Unfallort, dem Material und der Zahl der Unfallbeteiligten ist. Der Schaden kann sowohl sicherheitstechnische, finanzielle als auch umweltrelevante Folgen haben. Bei BP-Risk wird das Schadenspotenzial als Funktion der gefährdeten Personen, der Geschwindigkeit sowie der Zuggattung dargestellt. Dieser Ansatz besitzt den Vorteil, dass das Schadensausmaß (Parameter S) nicht mehr direkt geschätzt werden muss, sondern Subparameter verwendet werden, die einfacher geschätzt werden können.

BP-Risk

Im Folgenden werden für die explizite Risikoeinschätzung jeweils die einzelnen Gefährdungen aus Tabelle 10-3 bewertet. Im Rahmen der Analyse stellte sich heraus, dass gewisse Parameter für alle Gefährdungen den gleichen Wert haben, nämlich die Betriebsdichte (B) und die Zuggattung (T). Sie sind in der Regel von der Strecke und den darauf verkehrenden Zügen abhängig. Anhand der Systemdefinition und der oben getroffenen Annahmen für den ZLB können diese Parameter bereits bewertet werden, da sie für alle Zugleistrecken gelten.

Der Zugleitbetrieb wird auf Strecken mit einem starren Betriebsprogramm eingesetzt, bei dem ein Zugfolgeabstand von einer Stunde (und mehr) angenommen wird. Das bedeutet, es verkehren ca. 25 Züge pro Tag⁶⁶. Laut Streckenstandards (siehe Tabelle 6-3) ist dies die Obergrenze der Streckenauslastung für eine Regionalstrecke R 80. Da im Rahmen von BP-Risk für eine durchschnittliche Betriebsdichte eine Regionalverkehrsstrecke R 120 mit ca. 100 Zugpaaren pro Tag angenommen wurde, wird für den ZLB eine geringe Betriebsdichte (unterhalb des Netzdurchschnitts) angesetzt. Der Parameter B beträgt somit im Rahmen dieses Anwendungsbeispiels für alle Gefährdungen den Wert Eins (siehe Tabelle 10-4).

Tabelle 10-4 Parameter B für ZLB Beispiel

| B | Qualitative Beschreibung | Beispiele |
|---|--------------------------|--|
| 1 | Gering | Unter Netzdurchschnitt, z. B. auf Güterverkehrsstrecken |
| 2 | Normal | Netzdurchschnitt, z.B. auf Regionalverkehrsstrecke |
| 3 | Erhöht | Über Netzdurchschnitt, z. B. auf Fernverkehr- und HGV-Strecken |

Da eine Nebenbahn mit Personenverkehr betrachtet und der Güterverkehr vorerst nicht berücksichtigt wird, ist davon auszugehen, dass in der Regel Zuggattungen, wie Regionalbahnen auf Zugleistrecken zum Einsatz kommen (siehe auch Tabelle 6-6).

⁶⁶ Es gibt natürlich auch Zugleistrecken mit deutlich dichter Zugfolge (z.B. über 40 Züge/Tag). Ein Extremfall war über Jahre die zur AKN gehörende Alsternordbahn, auf der auf einer eingleisigen Strecke mit dichter Folge von Kreuzungsbahnhöfen ein 10 min-Takt gefahren wurde. Für solche Fälle müsste der Betriebsparameter im Rahmen von BP-Risk dementsprechend angepasst werden.

Die Gefährdungsszenarien sind unabhängig von den Zuggattungen, so dass ebenso ein konstanter Parameterwert für T angenommen werden kann. Dieser beträgt im Rahmen dieses Anwendungsbeispiels für alle Gefährdungen ebenfalls den Wert Eins (Tabelle 10-5).

Tabelle 10-5 Parameter T für ZLB Beispiel

| T | Qualitative Beschreibung | Beispiele |
|---|--------------------------|---|
| 1 | SPNV | Regional Bahn, Stadtexpress, S-Bahn Züge |
| 2 | SPFV + HGV | Triebzüge, bespannte Personenverkehrszüge, Nachtzüge, Autoreisezüge |
| 3 | SGV | Güterzüge (auch Schnellgüterzüge) |

Nachfolgend werden nun die verbleibenden Risikoparameter im Rahmen von BP-Risk für die jeweilige Gefährdung bewertet.

| Nr. | Gefährdung | Beteiligte | |
|-------------------------|--|------------|----------|
| G1 $\frac{a}{b}$ | Zustimmung zur Fahrt fälschlicherweise erteilt | Zl (Fdl) | Zf (Tf), |
| | | Zf (Tf) | |

Die Zustimmung zur Fahrt erfolgt fernmündlich mittels einer Fe durch den Zl an den Zf (bzw. Tf in Funktion des Zf). Gleiches gilt für den Fdl in Funktion des Zl. Bei Zugkreuzungen auf unbesetzten Zuglaufstellen holt der im Bahnhof stehende Zug den vor der Trapeztafel haltenden Zug in den Bahnhof durch das Signal „Kommen“ und erteilt somit die Zustimmung zur Einfahrt. Die Gefährdung ‚Zustimmung zur Fahrt fälschlicherweise erteilt‘ entsteht somit an der Schnittstelle zwischen Zl und benachbartem Fdl (an der Systemgrenze des ZLB), zwischen Zl und Zf und zwischen Zf und Zf bei Zugkreuzungen auf unbesetzten Zuglaufstellen. Die Gefährdung kann aus verschiedenen Gründen entstehen:

- falsche Überlegungen (z. B. Zulässigkeit der Fahrt fehlerhaft geprüft),
- Nichteinhaltung der Sprachdisziplin zwischen Fdl und Zl oder Zl und Zf,
- Fehlerhafte oder missverständliche Kommunikation,
- Fehlerhafte Eintragungen in den betrieblichen Unterlagen.

Die hier aufgeführten menschlichen Fehlhandlungen sind insbesondere für den Zl und den Zf entscheidend, denn bei Fehlhandlungen des benachbarten Fdl kann die üblicherweise vorhandene Sicherungstechnik die Folgen verhindern. Allerdings übernimmt der benachbarte Fdl an der Systemgrenze des ZLB Aufgaben des Zugleiters. Beispielsweise muss der benachbarte Fdl für den in die Zugleitstrecke einfahrenden Zug eine Fahrerlaubnis (Fe) bis zur nächsten Zuglaufstelle erteilen, bevor er der Ausfahrt mittels Fahrtstellung des Ausfahrsignals zustimmt. Das EBA hat im Rahmen einer Unfalluntersuchung (/57/) festgestellt, dass vor Erteilung des Abfahrauftrages im konkreten Fall regelmäßig keine Fe erteilt wurde. Auf Strecken ohne Streckenblock (wie oben für die Zugleitstrecke angenommen) kann ein Ausfahr-signal jederzeit auf Fahrt gestellt werden, selbst wenn ein Gegenzug kommt.

Das bedeutet, dass selbst die vorhandene Signaltechnik im Bahnhof nicht verhindern kann, dass der Zug ohne oder mit einer ungültigen Fe in die Zugleitstrecke einfährt.

Bei der Bewertung der menschlichen Handlungen muss beachtet werden, dass es beim ZLB eigentlich keine Rückfallebene gibt, bei dessen Anwendung sich das Betriebspersonal in einer nicht täglichen praktizierten Situation wiederfindet. Die Folgen aus Fehlhandlungen werden nicht durch technische Einrichtungen unterbunden. Deswegen sollte allen Beteiligten bewusst sein, dass die Betriebsabwicklung mit besonderer Aufmerksamkeit und hohem Verantwortungsbewusstsein durchgeführt werden muss. Auf Strecken mit ZLB gleicht sich die Betriebsabwicklung jedoch Tag für Tag. Es ist meist ein starrer Fahrplan mit immer wiederkehrenden Kreuzungen im selben Bahnhof vorhanden. Vielfach ist eine Kreuzungsverlegung im Verspätungsfall, bedingt durch die Abstände der Bahnhöfe, gar nicht möglich (nach /107/, Seite 69). Viele Beteiligte kennen sich persönlich, weil sie regelmäßig auf der Strecke Dienst haben. Allerdings birgt der Alltag die Gefahr der Gewohnheit und der Nachlässigkeiten bei der korrekten Durchführung der betrieblichen Handlungen.

Im Rahmen von BP-Risk muss unterschieden werden zwischen den menschlichen Handlungen, die Teil des Betriebsverfahrens sind, und den menschlichen Handlungen, die nach Eintreten der Gefährdung bzw. des Funktionsversagens zur Gefahrenabwehr zählen. Die menschlichen Handlungen, die zum Betriebsverfahren gehören, sind mindestens alle Handlungen, die im ZLB durch Regeln definiert sind (z. B. das Durchführen von Zuglaufmeldungen oder die Sicherung des Fahrwegs). Für die Beurteilung der Gefährdung G1 bedeutet dies, dass die ungültige Zustimmung zur Fahrt bereits erteilt wurde und nun zu bewerten ist, ob eine menschliche Gefahrenabwehr noch möglich ist. Dazu muss berücksichtigt werden, wer an der Funktion „Zustimmung zur Fahrt erteilen“ beteiligt ist.

Szenario a)

Wenn die Zuglaufmeldungen zwischen ZI und Zf ausgetauscht werden, ist dies gleichzusetzen mit der Situation, dass der ZI mit dem benachbarten Fdl kommuniziert. In beiden Fällen ist die betriebliche Kommunikation durch Regeln festgelegt. Wenn nun eine ungültige Zustimmung zur Fahrt erteilt wird, ist davon auszugehen, dass eine Offenbarung durch den anderen Gesprächspartner nicht mehr möglich ist. Die ungültige Fe wird dem Tf übermittelt und nur er hat die Möglichkeit durch Strecken- und Fahrplankenntnis eine falsche Fe aufzudecken. Nach Hinzen sind menschliche Handlungen wie Streckenkenntnis zwar fertigkeitstbasierende Handlungen, aber nur im Regelbetrieb. Das vorliegende Gefährdungsszenario erfordert eine Nothandlung des Tf. Es wird hierbei jedoch angenommen, dass ein geschulter Tf darauf trainiert wurde, eine erhaltende Fe am vorliegenden Buchfahrplan und aufgrund seiner Streckenkenntnis auf Plausibilität zu prüfen. Im vorliegenden Falle reicht eine einfache Rückfrage des Tf, um die ungültige Fe zu offenbaren. Somit wird für dieses Gefährdungsszenario die Gefahrenabwehr als häufig möglich eingestuft, was dem Wert $M = 1$ entspricht (siehe Tabelle 6-5).

Szenario b)

Im Falle einer Zugkreuzung, bei der die Variante 2 (siehe Abbildung 10-6) angewendet wird, ist der ZI nicht beteiligt, sondern nur die beiden Zugführer (oder ggf. Triebfahrzeugführer). Die Gefährdung liegt vor, wenn der Zf des ersten Zuges fälschlicherweise das Signal „Kommen“ gibt, was einer Zustimmung zur Fahrt gleichzusetzen ist. Die menschliche Gefahrenabwehr bewertet nun das Verhalten vom Tf des zweiten einfahrenden Zuges. Es wird angenommen, dass es für den Tf des zweiten Zuges noch möglich ist, rechtzeitig zu bremsen, da er i.d.R. mit einer geringen Geschwindigkeit den Bahnhof befährt (weil er vorher an der Trapeztafel gehalten hat) und dadurch mögliche Hindernisse noch rechtzeitig erkennen kann. Hierbei handelt es sich jedoch nicht um eine routinemäßige Handlung, sondern ebenfalls um eine Notreaktion. Somit wird für dieses Gefährdungsszenario die Gefahrenabwehr als selten möglich eingestuft, was dem Wert $M = 3$ entspricht (siehe Tabelle 6-5).

Im Rahmen von BP-Risk werden die maßgeblichen Geschwindigkeiten bewertet, die nach Gefährdungseintritt bzw. beim Unfall auftreten. Im Rahmen der Unfalluntersuchung eines Zusammenstoßes auf einer Zugleitstrecke (/57/) wurden maßgebliche Geschwindigkeiten von 39 km/h und 44 km/h gemessen. Dies würde für den Parameter V einen Wert von Eins ergeben (siehe Tabelle 6-8), da es sich bei den genannten Angaben um geringe Geschwindigkeiten handelt. Auf der betreffenden Zugleitstrecke betrug die Streckenhöchstgeschwindigkeit jedoch 50 km/h. Im Allgemeinen beträgt die oben angenommene Streckenhöchstgeschwindigkeit im ZLB bis zu 80 km/h. Daher wird für den Parameter V eine mittlere Geschwindigkeit auf der freien Strecke angenommen, was dem Wert $V = 2$ entspricht. Der mögliche Unfall kann natürlich auch im Bahnhof stattfinden, wo in der Regel mit niedrigeren Geschwindigkeiten als der Streckenhöchstgeschwindigkeit gefahren wird. Wenn die Kommunikation zwischen ZI und Zf nicht zustande kommt, darf nicht oder maximal auf Sicht gefahren werden. Da im Rahmen dieser Gefährdung jedoch nicht eindeutig bewertet werden kann, ob der mögliche Unfall im Bahnhof oder auf der freien Strecke stattfindet, wird hier zur sicheren Seite die höhere Geschwindigkeit auf der Strecke als maßgeblich angenommen.

Zur Bewertung der betroffenen Personen wird angenommen, dass eine fälschlicherweise erteilte Zustimmung zur Zugfahrt dazu führen kann, dass ein Zug in einen durch einen anderen Zug besetzten Abschnitt einfährt. Dies wiederum würde typischerweise zu einem Zusammenstoß dieser beiden Züge führen. Für Parameter A (siehe Tabelle 6-11) wird i. d. R. bei einem Zusammenstoß davon ausgegangen, dass sehr viele Personen betroffen sind (also mehrere Tote und Verletzte). Bei einem Zusammenstoß auf einer Zugleitstrecke im September 2003 (/57/) wurden jedoch ‚nur‘ 27 Personen verletzt. Daher werden für den Parameter A für die Folge eines Zusammenstoßes im ZLB ‚viele‘ (statt ‚sehr viele,‘) betroffene Personen angenommen ($A = 4$).

Insgesamt ergeben sich die Werte für

- Szenario G1 a): $G + S = 1 + 1 + 1 + 2 + 4 = 9$, und
- Szenario G1 b): $G + S = 1 + 3 + 1 + 2 + 4 = 11$.

Diese werden im Rahmen der Risikobewertung einer tolerierbaren Häufigkeit für diese Gefährdungsszenarien zugeordnet (siehe 10.2.4).

| Nr. | Gefährdung | Beteiligte | |
|-----------|--|----------------|-----------|
| G2 | Falsche/verfälschte Zuglaufmeldung gegeben | a | |
| b | | | |
| | | Zugführer (Tf) | Zugleiter |

Die Gefährdung ‚Falsche/verfälschte Zugmeldung gegeben‘ entsteht an der Schnittstelle zwischen Zf und Zl und vereint (wie oben erwähnt) mehrere Funktionsversagen. Durch die Zuglaufmeldungen werden im ZLB die betrieblichen Informationen übermittelt, wobei das korrekte Durchführen der Meldungen die Basis für eine sichere Betriebsführung ist. Gefährdung G1 ‚Zustimmung zur Fahrt fälschlicherweise erteilt‘ betrachtet auch eine Zuglaufmeldung, nämlich die Zustimmung zur Fahrt durch eine Fe. G1 betrachtet allerdings die Information, die bei Szenario a) vom Zugleiter (oder benachbarten Fdl) dem Zugführer übermittelt wird. Szenario b) berücksichtigt die Zustimmung zur Fahrt bei einer Zugkreuzung in einem unbesetzten Bahnhof ohne Rückfallweichen. Die vorliegende Gefährdung G2 betrachtet im Gegensatz zur Gefährdung G1 die betrieblichen Informationen (in Form von Zuglaufmeldungen), die in Szenario a) der Zugführer dem Zugleiter mitteilt, z. B. Ortungs- und Gleisfreimeldungen. Szenario b) betrachtet erneut den Fall der Zugkreuzung.

Die Funktion Ortung wird im ZLB durch Hinsehen (Streckenbeobachtung) und durch die Abgabe einer Ankunfts- oder Verlassensmeldung oder Abstellmeldung durch den Zugführer an den Zugleiter ausgeführt. Die Funktion Gleisfreimeldung erfolgt im ZLB durch die Abgabe einer Ankunfts- oder Verlassensmeldung, Fahrwegsicherungsmeldung oder Abstellmeldung durch den Zugführer an den Zugleiter (Szenario a) oder durch das Signal „Kommen“ bei Zugkreuzungen auf unbesetzten Zuglaufstellen (Szenario b).

Die Gefährdung ‚Falsche/verfälschte Zugmeldung gegeben‘ kann folgende Ursachen haben:

- falsche Überlegungen (z. B. Zugnummer vertauscht),
- Nichteinhaltung der Sprachdisziplin zwischen Fdl und Zl oder Zl und Zf,
- fehlerhafte oder missverständliche Kommunikation,
- fehlerhafte Eintragungen in den betrieblichen Unterlagen (z. B. falsche Weg- oder Geschwindigkeitsinformationen).

Die fernmündliche Übermittlung von Zuglaufmeldungen gehört zu den menschlichen Handlungen, die Teil des Betriebsverfahrens ZLB sind. Zur Beurteilung der menschlichen Gefahrenabwehr für die Gefährdung G2 muss nun bewertet werden, inwiefern es möglich ist, nach einer falschen oder verfälschten Zuglaufmeldung einen Unfall noch zu verhindern. Dazu muss, wie bei der Gefährdung G1, berücksichtigt werden, wer an der Funktion beteiligt ist. Es werden dazu, wie bei Gefährdung G1, zwei Szenarien unterschieden.

Szenario a)

Wenn die oben genannten Zuglaufmeldungen vom Zf mit falschen Informationen an den ZI übermittelt werden bzw. wenn durch die technische Einrichtung die Meldung verfälscht wird, hat der ZI kaum eine Möglichkeit, diese falschen Informationen zu offenbaren. Im bereits erwähnten Unfall auf einer Zugleitstrecke (/57/) vergaß der Zf eine Ankunfts meldung zu geben und eine erneute Fe anzufragen. Der ZI konnte in diesem Fall das Versäumnis nicht bemerken. Es ist in anderen Fällen sicherlich noch selten möglich, beispielsweise vertauschte Zugnummern oder falsche Ortungsmeldungen durch Plausibilitätschecks mit dem Fahrplan zu erkennen. Es wird jedoch davon ausgegangen, dass eine realistische Offenbarung von falschen Informationen entweder kaum oder gar nicht möglich ist. Somit wird für dieses Gefährdungsszenario die menschliche Gefahrenabwehr als fast nie möglich eingestuft, was dem Wert $M = 5$ entspricht (siehe Tabelle 6-5).

Szenario b)

Im Falle einer Zugkreuzung auf unbesetzten Zuglaufstellen ohne Rückfallweichen erfolgt die Gleisfreimeldung entweder durch eine Fahrwegsicherungsmeldung oder durch das Signal „Kommen“ vom zuerst eingefahrenen Zug. Eine falsche oder verfälschte Fahrwegsicherungsmeldung kann der ZI nicht offenbaren (siehe Szenario a). Wenn fälschlicherweise das Signal „Kommen“ gegeben wurde, wird wie bei Gefährdung G1 angenommen, dass der Tf des zweiten Zuges bei einem möglichen Hindernis im Bahnhof noch rechtzeitig bremsen kann, da von einer geringen Geschwindigkeit ausgegangen wird. Hierbei handelt es sich um eine Nothandlung des Tf, für die die menschliche Gefahrenabwehr als selten möglich eingestuft wird ($M = 3$).

Zuglaufmeldungen werden i. d. R. in der Zuglaufstelle gegeben, wobei die Verlassensmeldung die einzige Zuglaufmeldung ist, die während der Fahrt abgegeben werden darf. Die maßgebliche Geschwindigkeit nach Gefährdungseintritt ist schwer abzuschätzen, da ein möglicher Unfall sowohl auf der freien Strecke als auch im Bahnhof stattfinden kann.

Analog zu Gefährdung G1 wird daher für den Parameter V eine mittlere Geschwindigkeit als maßgeblich angenommen, was dem Wert $V = 2$ entspricht (siehe Tabelle 6-8).

Eine falsche Ortungs- oder Gleisfreimeldung und auch eine falsche Zugnummer können vorerst zu falschen Eintragungen in den betrieblichen Unterlagen des ZI führen. Diese Eintragungen wiederum bilden die Grundlage für den ZI zur Vergabe einer Fe. Somit könnte aufgrund von falschen Informationen aus einer Zuglaufmeldung eine ungültige Fe erteilt werden, was wiederum dazu führen kann, dass ein Zug in einen besetzten Abschnitt einfährt. Dies gilt auch für das Szenario einer Zugkreuzung (Szenario b). Wenn eine falsche FsE oder ein fälschlicherweise gegebenes Signal „Kommen“ gegeben wird, kann folglich ein Zug in einen besetzten Abschnitt einfahren. In Anlehnung an die Gefährdung G1 werden für einen möglichen Zusammenstoß auf einer Zugleitstrecke viele betroffene Personen angenommen, was nach Tabelle 6-11 einem Wert von $A = 4$ entspricht. Natürlich ist es auch möglich, dass der

besetzte Abschnitt nicht durch einen anderen Zug, sondern durch ein Hindernis besetzt ist, was einen Aufprall zur Folge hätte, bei dem i. d. R. weniger Personen betroffenen sind. In diesem Fall wird jedoch die ungünstigere Folge eines Zusammenstoßes angenommen, um auf der sicheren Seite zu bleiben.

Insgesamt ergeben sich die Werte für:

- Szenario G2 a): $G + S = 1 + 5 + 1 + 2 + 4 = 13$, und
- Szenario G2 b): $G + S = 1 + 3 + 1 + 2 + 4 = 11$.

Diese werden im Rahmen der Risikobewertung einer tolerierbaren Häufigkeit für diese Gefährdungsszenarien zugeordnet (siehe 10.2.4).

| Nr. | Gefährdung | Beteiligte | |
|-----|---|------------|----------|
| G3 | Fahrgrenzen nicht oder fehlerhaft überwacht | Tf | Fahrzeug |

Die Funktion Zugsicherung (Zugbeeinflussung) wurde aufgeteilt in die Funktionen ‚Fahrgrenzen überwachen‘ und ‚Geschwindigkeit überwachen‘. Im Rahmen von Gefährdung G3 wird nur das Funktionsversagen ‚Fahrgrenzen nicht oder fehlerhaft überwacht‘ bewertet. G4 betrachtet dann die fehlende oder falsche Überwachung der zulässigen Geschwindigkeit. Die Einhaltung der Fahrgrenzen ist Aufgabe des Tf. Grundlage dafür sind die Weginformationen, die über nicht stellbare Signale, über den Buchfahrplan bzw. über schriftliche Befehle des ZI übermittelt werden. Auch die Fahrerlaubnis (Fe) erhält Weginformationen, da sie als Ziel eine Zuglaufstelle nennt.

Die Gefährdung ‚Fahrgrenzen nicht oder fehlerhaft überwacht‘ kann sowohl auf der freien Strecke als auch im Bahnhof stattfinden. Das in der empirischen Phase der Gefährdungsidentifikation genannte Ereignis ‚Tf fährt ohne Fahrerlaubnis‘ findet sich in dieser Gefährdung G3 wieder. Das Fahren ohne Fahrerlaubnis hat als Ursache die fehlende Überwachung der Fahrgrenzen. Im vorliegenden Fall steht dem Tf dafür keine Sicherungstechnik zur Verfügung, um seine Fehlhandlungen aufzudecken und die möglichen Folgen zu verhindern.

Die Gefährdung kann entweder durch Fehlhandlungen des Triebfahrzeugführers entstehen oder durch das fehlende bzw. falsche Bereitstellen von Weginformationen (z. B. Halt- oder Trapeztafel stehen an falscher Stelle, falscher Eintrag im Buchfahrplan, fehlerhafter Befehl vom ZI). Fehlende oder falsche Weginformationen bilden im ZLB sicherlich die Ausnahme. Außerdem wäre der Tf durch seine Streckenkenntnis wohl in der Lage, diese Fehlinformationen schnell aufzudecken. Nach Hinzen sind menschliche Handlungen wie das ‚Bemerken und Beachten des Halt-zeigenden Signals‘, bzw. ‚Zuordnung von Signalen zu Gleisen und Bedeutung durch den Tf‘ Beispiele für fertigkeiten-basierende Handlungen im Regelbetrieb (siehe 6.1.2).

Die menschliche Gefahrenabwehr bewertet nun die Möglichkeit, nach dem Gefährdungseintritt einen Unfall noch zu verhindern. Wenn also der Tf die Fahrgrenzen nicht überwacht

(z. B. weil er eingeschlafen ist), ist es sehr fraglich, ob er seine eigene Fehlhandlung noch rechtzeitig bemerken kann, um einzugreifen. Daher wird die menschliche Gefahrenabwehr als fast nie möglich eingestuft, was einem Wert von $M = 5$ (siehe Tabelle 6-5) entspricht.

Als typische Folge der Gefährdung kann angenommen werden, dass der betrachtete Zug in einen möglicherweise durch einen anderen Zug besetzten Abschnitt einfährt. Da im Rahmen dieser Gefährdung nicht eindeutig bewertet werden kann, ob ein mögliches Zusammentreffen dieser beiden Züge im Bahnhof oder auf der freien Strecke stattfindet, wird hier die Geschwindigkeit auf der Strecke als maßgeblich angenommen, was dem Wert $V = 2$ entspricht (siehe Tabelle 6-8). Wie bei den vorangegangenen Gefährdungen werden für den Fall eines möglichen Zusammenstoßes viele betroffene Personen angenommen, was nach Tabelle 6-11 dem Wert $A = 4$ entspricht.

Insgesamt ergibt sich für BP-Risk der Wert: $G + S = 1 + 5 + 1 + 2 + 4 = 13$. Dieser wird im Rahmen der Risikobewertung einer tolerierbaren Häufigkeit für diese Gefährdung zugeordnet (siehe 10.2.4).

| Nr. | Gefährdung | Beteiligte | |
|-----|---|------------|----------|
| G4 | Geschwindigkeit nicht oder fehlerhaft überwacht | Tf | Fahrzeug |

Die Einhaltung der zulässigen Geschwindigkeit ist die Aufgabe des Tf. Grundlage dafür sind die Geschwindigkeitsinformationen des Fahrzeugs (Ist-Geschwindigkeit) und die Geschwindigkeitsinformationen im Buchfahrplan oder über schriftliche Befehle (Soll-Geschwindigkeit). Die Gefährdung ‚Geschwindigkeit nicht oder fehlerhaft überwacht‘ kann sowohl auf der freien Strecke als auch im Bahnhof stattfinden.

Die Gefährdung kann entweder durch Fehlhandlungen des Triebfahrzeugführers entstehen oder durch fehlende bzw. falsche Bereitstellung von Geschwindigkeitsinformationen (z. B. durch falsche Einträge im Buchfahrplan, falscher Befehl vom ZI, falsche Geschwindigkeitsanzeige im Tfz). Wie bei der Gefährdung G3 wird angenommen, dass die falsch bereitgestellten Geschwindigkeitsinformationen im Vergleich zu den menschlichen Fehlhandlungen die Ausnahme bilden. Und auch in einem solchen Ausnahmefall kann davon ausgegangen werden, dass der Tf durch seine Streckenkenntnis in der Lage wäre, diese Fehlinformationen schnell aufzudecken.

Wenn jedoch der Tf die Geschwindigkeit nicht oder fehlerhaft überwacht, ist anzunehmen, dass es keine Möglichkeit gibt, der eigenen Fehlhandlung noch rechtzeitig entgegenzuwirken. Das Funktionsversagen wird dann erst durch den daraus resultierenden Unfall offenbart. Wie bei Gefährdung G3 wird deshalb die menschliche Gefahrenabwehr als fast nie möglich eingestuft, was einem Wert von $M = 5$ (siehe Tabelle 6-5) entspricht.

Als mögliche Folge der Gefährdung kann angenommen werden, dass der betrachtete Zug mit zu hoher Geschwindigkeit fährt. Da auch im Rahmen dieser Gefährdung nicht eindeutig

bewertet werden kann, ob dies im Bahnhof oder auf der freien Strecke passiert, wird hier die Geschwindigkeit auf der Strecke als maßgeblich angenommen ($V = 2$).

Bei überhöhter Geschwindigkeit wird eine Entgleisung als typische Unfallfolge angenommen. In Weichenbereichen sind Entgleisungen sicherlich realistisch, aber auf der freien Strecke bliebe zu klären, ob bei geringen Geschwindigkeiten, wie sie im ZLB vorkommen, Entgleisungen überhaupt möglich sind. Wenn von einer Entgleisung ausgegangen werden kann, können nach Tabelle 6-11 einige betroffene Personen angenommen werden. Dies entspricht dem Wert $A = 3$.

Insgesamt ergibt sich für BP-Risk der Wert: $G + S = 1 + 5 + 1 + 2 + 3 = 12$. Dieser wird im Rahmen der Risikobewertung einer tolerierbaren Häufigkeit für diese Gefährdung zugeordnet (siehe 10.2.4).

| Nr. | Gefährdung | Beteiligte | |
|-------------------------|---|----------------|---------|
| G5 $\frac{a}{b}$ | Fahrweg nicht oder fehlerhaft eingestellt | Zugführer (Tf) | Fahrweg |

Der Fahrweg wird bei Kreuzungen auf unbesetzten Betriebsstellen ohne Rückfallweichen bzw. bei Überholungen auf unbesetzten Betriebsstellen durch den Zf des zuerst eingefahrenen Zuges eingestellt. Nach Verlassen einer unbesetzten Betriebsstelle ohne Rückfallweichen stellt der Zf die Grundstellung wieder her. Die Gefährdung ‚Fahrweg nicht oder fehlerhaft eingestellt‘ kann demnach entstehen bei einer Zugkreuzung im Bahnhof, wenn in unbesetzten Bahnhöfen das Zugpersonal den Fahrweg für den zweiten Zug einstellen und sichern muss (siehe Kapitel 10.1.2). Die Fahrwegsicherung wird in Gefährdung G6 betrachtet, hier geht es vorerst nur um die korrekte Einstellung des Fahrweges.

Wie bei den Annahmen für den ZLB festgelegt, wird hier ein unbesetzter Bahnhof betrachtet, der ohne Rückfallweichen oder sonstige Technik (z. B. ortsgestellte Weichen) ausgestattet ist. Der zuerst eingefahrene Zug muss also für den zweiten Zug die Weichen umstellen. Die Gefährdung kann eigentlich nur aus falschen Überlegungen des Zugpersonals entstehen, z. B. wenn das Zugpersonal vergisst den Fahrweg einzustellen oder wenn die eigene Ausfahrt gestellt wird, obwohl der kreuzende Zug noch in das andere Gleis einfahren soll.

Zur Beurteilung der menschlichen Gefahrenabwehr werden wiederum zwei unterschiedliche Gefährdungsszenarien unterschieden, nämlich das Einstellen des Fahrwegs für den zweiten Zug (Szenario a) und das Herstellen der Grundstellung für die Weiterfahrt des ersten Zuges (Szenario b).

Szenario a)

Für die menschliche Gefahrenabwehr muss nun bewertet werden, inwiefern der Tf des zweiten Zuges den nicht oder fehlerhaft eingestellten Fahrweg erkennen und er seinen Zug noch bremsen kann. Nach Hinzen ist die Beobachtung, ob Weichen richtig stehen, eine fertigkeits-

basierende Handlung, da sie routinemäßig abläuft (siehe Kapitel 6.1.2). Hierbei ist jedoch zu beachten, dass Triebfahrzeugführer von Zügen nicht zur Weichenbeobachtung verpflichtet sind, nicht einmal beim Fahren auf Sicht. Es wird davon ausgegangen, dass einem Zug immer ein richtig eingestellter Fahrweg garantiert wird.

In der Regel ist mit der Stellvorrichtung von Weichen auch ein Weichensignal verbunden, das die Lage der Weiche erkennbar macht (dies entspricht einer technischen Lösung). Weichensignale sollen somit Unfälle aufgrund falscher Weichenstellung verhindern. Die Weichensignale werden i.d.R. jedoch nur zum Rangieren gebraucht. Es ist fraglich, ob bei einer niedrigen Signallaterne der Weichensignale die rechtzeitige Erkennung einer falschen Weichenlage überhaupt möglich ist⁶⁷. Da Züge auch lange Bremswege besitzen, gibt es bestenfalls bei geringen Geschwindigkeiten (z. B. bei Rangierfahrten) eine echte Chance durch Weichensignale, Unfälle zu vermeiden. Im vorliegenden Fall kann von einer geringen Einfahrtgeschwindigkeit des zweiten Zuges in den Bahnhof ausgegangen werden, da dieser vorher an der Trapeztafel gehalten hat. Insofern könnte eine menschliche Gefahrenabwehr noch möglich sein ($M = 3$).

Szenario b)

Hat der zweite Zug den Bahnhof verlassen, muss das Zugpersonal des ersten Zuges die Weichen wieder in Grundstellung bringen, da dies die Voraussetzung für die eigene Weiterfahrt ist. Wenn in diesem Fall das Zugpersonal den Fahrweg nicht oder fehlerhaft einstellt, ist es sehr fraglich, ob die eigene Fehlhandlung noch bemerkt und offenbart werden kann. Somit wäre hierfür die menschliche Gefahrenabwehr als fast nie möglich einzustufen ($M = 5$).

Die typische Folge bei einem nicht oder falsch eingestellten Fahrweg wäre typischerweise, dass ein Zug in ein falsches und möglicherweise besetztes Gleis oder einen besetzten Abschnitt einfährt. Da das Einstellen des Fahrwegs in Bahnhöfen (Zuglaufstellen) stattfindet, kann angenommen werden, dass sich ein möglicher Unfall auch dort ereignen würde.

Wie bereits oben erwähnt, wird davon ausgegangen, dass im Bahnhof mit niedrigeren Geschwindigkeiten als der Streckenhöchstgeschwindigkeit (max. 80 km/h) gefahren wird. Dies kann auch damit begründet werden, dass laut EBO (§§14 und 15) für Nebenbahnen auf gewisse Streckenausrüstung verzichtet werden kann, z. B. auf

- „Einfahrtsignale bei einer Einfahrtgeschwindigkeit bis 50 km/h,
- Ausfahrtsignale bei Ausfahrtgeschwindigkeiten bis 60 km/h,
- Signalabhängigkeit von Weichen bei Geschwindigkeiten bis 50 km/h“ (/107/, S. 14).

⁶⁷ Eine Ausnahme sind Rückfallweichen, deren Überwachungssignale als hohe Signale ausgeführt sind und die mit Bakken angekündigt werden. Rückfallweichen werden hier jedoch nicht berücksichtigt, da sie bereits eine technische Realisierung darstellen.

Für die Gefährdung G5 wird also von einer geringen maßgeblichen Geschwindigkeit ausgegangen, die nach Tabelle 6-8 dem Wert $V = 1$ entspricht.

Zur Bewertung der betroffenen Personen wird angenommen, dass eine Fahrt in ein durch einen anderen Zug besetztes Gleis oder in einen besetzten Abschnitt zu einem Zusammenstoß führen kann. Eine Entgleisung wäre bei einem nicht oder falsch eingestellten Fahrweg auch möglich, wenn der Zug unerlaubt mit einer zu hohen Geschwindigkeit eine fälschlicherweise abzweigende Weiche befährt. Zur sicheren Seite wird hier die ungünstigere Variante angenommen, so dass davon ausgegangen wird, dass viele Personen betroffen wären. Dies entspricht dem Wert $A = 4$ (siehe Tabelle 6-11).

Insgesamt ergeben sich die Werte für:

- Szenario G5 a): $G + S = 1 + 3 + 1 + 1 + 4 = 10$, und
- Szenario G5 b): $G + S = 1 + 5 + 1 + 1 + 4 = 12$.

Diese werden im Rahmen der Risikobewertung einer tolerierbaren Häufigkeit für diese Gefährdungsszenarien zugeordnet (siehe 10.2.4).

| Nr. | Gefährdung | Beteiligte | |
|-----|---|----------------|---------|
| G6 | Fahrweg nicht oder fehlerhaft gesichert | Zugführer (Tf) | Fahrweg |

Die Sicherung des Fahrwegs wird durch den Zf i.d.R. durch das Verschließen der Weichen oder der Hebelbank durchgeführt. Die Gefährdung ‚Fahrweg nicht oder fehlerhaft gesichert‘ kann entstehen bei einer Zugkreuzung im Bahnhof, wenn in unbesetzten Bahnhöfen das Zugpersonal den Fahrweg für den zweiten Zug einstellen und sichern muss (siehe Kapitel 10.1.2). Die Einstellung des Fahrweges wurde in Gefährdung G5 betrachtet, hier geht es nun um die Sicherung des Fahrwegs.

Wie bei Gefährdung G5 wird ein unbesetzter Bahnhof betrachtet, der ohne Rückfallweichen oder sonstige Technik (z. B. ortsgestellte Weichen) ausgestattet ist. Der zuerst eingefahrene Zug muss für den zweiten Zug die Weichen sichern. Dies sind i. d. R. Handweichen, die in Grundstellung verschlossen sind (Handverschluss). Der Zf des ersten Zuges führt den Zugführerschlüssel mit sich und kann somit die Weichen umstellen und wieder verschließen.

Der Weichenverschluss⁶⁸ ist in der Regel so konstruiert, dass die Weiche mit geringer Geschwindigkeit ($v \leq 40$ km/h) vom Herzstück her aufgefahren werden kann (die falsch liegende Weiche wird stumpf befahren), ohne dass dieses zu einer Entgleisung oder Beschädigung führt.

⁶⁸ Einrichtung, durch die Weichenzungen und bewegliche Herzstückspitzen formschlüssig festgehalten werden (/95/). Nicht zu verwechseln mit dem Handverschluss, der für den Verschluss der Weichenstelleinrichtung zuständig ist!

Die Gefährdung kann aus falschen Überlegungen des Zugpersonals entstehen, z. B. wenn das Zugpersonal vergisst den Fahrweg zu sichern oder die Weichen nicht richtig verschließt. Für die Einstufung der Gefahrenabwehr wird bewertet, inwiefern der Tf des zweiten Zuges den nicht gesicherten Fahrweg erkennen kann, um möglicherweise noch rechtzeitig eingreifen zu können. Die Frage ist, inwieweit eine nicht gesicherte Weiche überhaupt erkennbar ist für den zweiten Zug – selbst bei geringen Einfahrtgeschwindigkeiten und ggf. vorhandenen Weichensignalen. Außerdem ist die Fahrwegsicherung nach Verlassen des zweiten Zuges auch für den ersten Zug durchzuführen. Dort ist es ebenfalls fraglich, ob eine falsch ausgeführte Sicherung überhaupt durch den Durchführenden bei Abfahrt offenbart werden kann. In beiden Fällen wird die menschliche Gefahrenabwehr als fast nie möglich angenommen, was einem Wert von Wert M = 5 (siehe Tabelle 6-5) entspricht.

Da das Einstellen und Sichern des Fahrwegs in Bahnhöfen (Zuglaufstellen) stattfindet, wird wie bei G5 angenommen, dass sich ein möglicher Unfall im Bahnhofsbereich ereignen würde. Daher wird auch hier von einer geringen maßgeblichen Geschwindigkeit ausgegangen ($V = 1$).

Eine mögliche Folge der Gefährdung wäre, dass die Weiche unter dem fahrenden Zug umlaufen könnte, wenn sie nicht richtig verschlossen wurde. Das Umstellen einer ortsgestellten Weiche unter dem fahrenden Zug ist allerdings nach Expertenschätzung sehr unwahrscheinlich, da dies mit einer großen Verletzungsgefahr für den Weichenbediener verbunden ist und es ein erhebliches Maß an Böswilligkeit voraussetzt. Außerdem ist in Anwesenheit des Zugführers des ersten Zuges auszuschließen, dass Dritte versuchen könnten, eine Weiche unter dem Zug umzustellen⁶⁹. Somit bliebe als realistische Folge für Gefährdung G6 nur das eigentliche Vergessen der Weichensicherung. Wobei bei geringen Geschwindigkeiten (wie oben angenommen) zu klären ist, ob eine Entgleisung überhaupt möglich ist. Es wird hier vorerst angenommen, dass es beim Vergessen der Fahrwegsicherung zu einer Entgleisung des Zuges kommen kann. Daher werden für den Parameter A (nach Tabelle 6-11) für die Folge einer Entgleisung einige betroffene Personen angenommen ($A = 3$). Insgesamt ergibt sich der Wert: $G + S = 1 + 5 + 1 + 1 + 3 = 11$. Dieser wird im Rahmen der Risikobewertung einer tolerierbaren Häufigkeit für diese Gefährdung zugeordnet (siehe 10.2.4).

⁶⁹ Daher wird bei spitz befahrenen ortsgestellten Weichen auf einen Handverschluss verzichtet, wenn die Weichen mit einem Hebelgewicht ausgerüstet sind und vom Bediener überblickt und gegen unberechtigten Eingriff geschützt werden können (KoRil 408.0601, Abschnitt 1 Handverschluss, Darstellung (2), Fall b)). Bei stumpf befahrenen ortsgestellten Weichen wird sogar immer auf einen Handverschluss verzichtet.

10.2.4 Risikobewertung

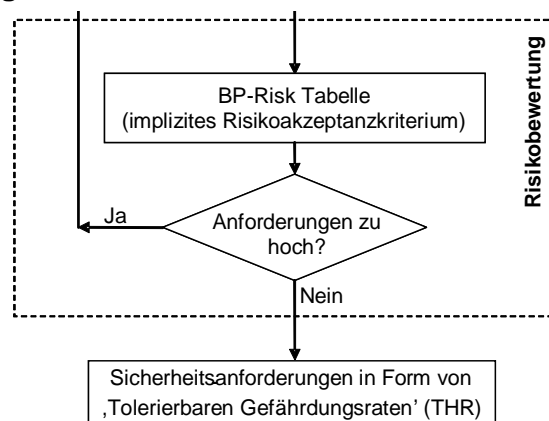


Abbildung 10-12 Risikobewertung mit BP-Risk

Im Rahmen der Risikobewertung sollen nach dem ERA-Prozess mit Hilfe der Risikoakzeptanzgrundsätze (hier: explizite Risikoeinschätzung) mögliche Sicherheitsmaßnahmen ermittelt werden, mit denen die Risiken des zu bewertenden Systems auf ein vertretbares Maß beschränkt werden. Ziel ist es, durch Vergleich der Analyseergebnisse mit dem gewählten Risikoakzeptanzkriterium systematisch und nachvollziehbar zu einer tolerierbaren Gefährdungsrate (THR) zu kommen. Die Risikobewertung dient dabei der Definition der THR für die Gefährdungen an der Systemgrenze und der Überprüfung, ob die zugehörigen Risiken tolerierbar sind. Die explizite Bestimmung von Risiken ist im Rahmen von BP-Risk nicht erforderlich. Die Risikobewertung erfolgt anhand der BP-Risk-Tabelle zur Ableitung der zulässigen Häufigkeit für eine Systemgefährdung (Tabelle 7-6), die anhand des europäischen Risikoakzeptanzkriterium nach /113/ kalibriert wurde.

Tabelle 10-6 zeigt zusammenfassend die Bewertung der einzelnen Gefährdungen sowie deren mit Hilfe von Tabelle 7-6 ermittelten THR-Werte. Dabei bedeutet eine THR von beispielsweise $3 \cdot 10^{-5}/h$, dass die Gefährdung einmal in 3 Jahren auftreten darf, damit sie tolerierbar bleibt. Für eine THR von $3 \cdot 10^{-7}/h$ gilt dies für einmal in 300 Jahren.

Insgesamt wird deutlich, dass die THR für die jeweiligen Gefährdungen des ZLB relativ nahe beieinander liegen, da die Gefährdungen sich nur in den Parametern ‚menschliche Gefahrenabwehr‘, ‚maßgebliche Geschwindigkeit‘ und ‚betroffene Personen‘ unterscheiden. Dies liegt unter anderem an den generischen Funktionen und somit generischen Gefährdungen, als auch an der gewollten realisierungs- und streckenunabhängigen Bewertung im Rahmen der expliziten Risikoeinschätzung. Es ist somit zu beachten, dass die resultierende THR der jeweiligen Gefährdung den Bezug ‚pro Funktion‘ hat und es sich dabei um Funktionen handelt, die Mensch und Technik umfassen. Die Realisierung, ob die Funktion nun strecken- oder fahrzeugseitig bzw. allein vom Menschen oder von der möglichen Unterstützungstechnik umgesetzt wird, ist hiermit noch offen und obliegt der Designfreiheit.

Tabelle 10-6 Ergebnisse der Risikobewertung

| | | B | M | T | V | A | G+S | THR |
|-----------|--|---|--------|---|---|---|----------|------------------|
| G1 | Zustimmung zur Fahrt fälschlicherweise erteilt Betriebsdichte: gering menschl. Gefahrenabwehr: häufig möglich (Szenario a) menschl. Gefahrenabwehr: selten möglich (Szenario b) Zuggattung: SPNV maßgebliche Geschwindigkeit: mittel betroffene Personen: viele | 1 | 1 3 | 1 | 2 | 4 | 9 11 | 3,E-05 3,E-06 |
| G2 | Zuglaufmeldung falsch/verfälscht gegeben Betriebsdichte: gering menschl. Gefahrenabwehr: fast nie möglich (Szenario a) menschl. Gefahrenabwehr: selten möglich (Szenario b) Zuggattung: SPNV maßgebliche Geschwindigkeit: mittel betroffene Personen: viele | 1 | 5 3 | 1 | 2 | 4 | 13 11 | 3,E-07 3,E-06 |
| G3 | Fahrgrenzen nicht/fehlerhaft überwacht Betriebsdichte: gering menschl. Gefahrenabwehr: fast nie möglich Zuggattung: SPNV maßgebliche Geschwindigkeit: mittel betroffene Personen: viele | 1 | 5 | 1 | 2 | 4 | 13 | 3,E-07 |
| G4 | Geschwindigkeit nicht/fehlerhaft überwacht Betriebsdichte: gering menschl. Gefahrenabwehr: fast nie möglich Zuggattung: SPNV maßgebliche Geschwindigkeit: mittel betroffene Personen: einige | 1 | 5 | 1 | 2 | 3 | 12 | 1,E-06 |
| G5 | Fahrweg nicht/fehlerhaft eingestellt Betriebsdichte: gering menschl. Gefahrenabwehr: selten möglich (Szenario a) menschl. Gefahrenabwehr: fast nie möglich (Szenario b) Zuggattung: SPNV maßgebliche Geschwindigkeit: gering betroffene Personen: viele | 1 | 3 5 | 1 | 1 | 4 | 10 12 | 1,E-05 1,E-06 |
| G6 | Fahrweg nicht/fehlerhaft gesichert Betriebsdichte: gering menschl. Gefahrenabwehr: fast nie möglich Zuggattung: SPNV maßgebliche Geschwindigkeit: gering betroffene Personen: einige | 1 | 5 | 1 | 1 | 3 | 11 | 3,E-06 |

10.3 Ergebnisse

Der Zugleitbetrieb ist ein Betriebsverfahren, bei dem die Sicherheit ausschließlich auf der Kommunikation zwischen Zugleiter und Zugpersonal und auf dem korrekten Führen der betrieblichen Unterlagen basiert. Eine Technik, die das menschliche Handeln überwacht und Fehlhandlungen erkennt und unterbindet, ist in der Regel nicht vorhanden. Die Sicherheit hängt einzig von der Einhaltung des Fahrplans und von der exakten Einhaltung der sicherheitsrelevanten Handlungsweise des Zugleiters und des Zugpersonals ab. Um die Sicherheit im Zugleitbetrieb zu erhöhen, ist es nötig, dass technische Einrichtungen die menschlichen Handlungen überwachen und kontrollieren. Dadurch können Gefährdungen erkannt und offenbart werden, indem beispielsweise die Ausführung von menschlichen Fehlhandlungen unterbunden wird. Dabei sind jedoch die wirtschaftlichen Investitionskosten gerade für Nebenbahnen zu berücksichtigen. Folglich *„müssen [diese technischen Systeme] also auch aufgrund der geringen Anforderungen der Strecken (einfache betriebliche Verhältnisse) und des besonderen Betriebsverfahrens unter den Anforderungen einer Signaltechnik bleiben. Sie müssen kostengünstig sein, um für Zugleitbetrieb Strecken attraktiv zu sein und dabei auch eine Alternative zum nächst höherwertigen Betriebsverfahren, dem Signalisierten Zugleitbetrieb, darzustellen“* (/107/, Seite 74).

Im Rahmen der Risikobeurteilung mit Hilfe von BP-Risk wurden Anforderungen für eine solch einfache unterstützende Technik zur Verbesserung der Sicherheit im ZLB abgeleitet. Die resultierenden Sicherheitsanforderungen gelten pro Stunde und pro Funktion und liegen im Mittel bei einer THR von $5,7 \cdot 10^{-6}/h$. Dies entspricht der Größenordnung, die in /107/ (Seite 76) als Gesamtfehlerwahrscheinlichkeit zur Erhöhung der Sicherheit im ZLB genannt wird, wobei zu beachten ist, dass es sich hierbei um keine Rate, sondern um eine Wahrscheinlichkeit handelt.

Es ist schwierig zu beurteilen, inwiefern der ZLB, wie er heute eingesetzt wird, die durch BP-Risk abgeleiteten Anforderungen erfüllt, da nach Kenntnisstand der Autorin bislang keine generischen Sicherheitsbetrachtungen zum ZLB vorliegen, die diese Werte belegen oder auch widerlegen könnten. Um jedoch eine vergleichbare Rate abzuleiten, wird im Folgenden beispielhaft anhand eines Fehlerbaums eine tolerierbare Gefährdungsrate ‚heruntergebrochen‘.

Wenn nun die einzusetzende Technik unabhängig von den menschlichen Handlungen ist, dann besteht im Rahmen eines Fehlerbaums eine ‚UND‘-Verknüpfung und die Ausfall- bzw. Fehlerwahrscheinlichkeiten dürfen multipliziert werden (siehe auch Kapitel 7.3). Die Unabhängigkeit der beiden Teilsysteme (Mensch und Technik) beim ZLB bedeutet, dass das Betriebsverfahren in vollem Umfang beibehalten wird und die Technik nur als Unterstützung dient. Es ist wichtig, dass der Mensch sich dabei nicht auf die technischen Einrichtungen verlassen darf, weil sonst die Gefahr besteht, dass er beispielsweise bei den betrieblichen Meldungen nachlässig wird.

Die Anforderung für eine solch einfache Unterstützungstechnik kann also mit Hilfe eines Fehlerbaums berechnet werden⁷⁰. Dies wird für die Gefährdung ‚Fahrgrenzen nicht/fehlerhaft überwacht‘ gezeigt, für die eine THR von $3 \cdot 10^{-7}/h$ pro Funktion ermittelt wurde. Zur Beherrschung dieser Gefährdung könnte z. B. eine punktförmige Zugbeeinflussung (PZB) eingesetzt werden, die eine unzulässige Vorbeifahrt an einer H-Tafel erkennt und eine sofortige Zwangsbremmung auslöst. Diese Möglichkeit empfiehlt die VDV-Schrift 752 als Mindestanforderung an technischer Unterstützung (siehe auch Anhang G: VDV-Schrift 752). In /107/ (Kapitel 6) werden verschiedene andere Möglichkeiten zur technischen Unterstützung des Zugleitbetriebs genannt und miteinander verglichen.

Das allgemeine Modell für das zu betrachtende Gefährdungsszenario ist in Abbildung 10-13 dargestellt (siehe auch Exkurs Gefährdungsdauer in Kapitel 5.3.1).

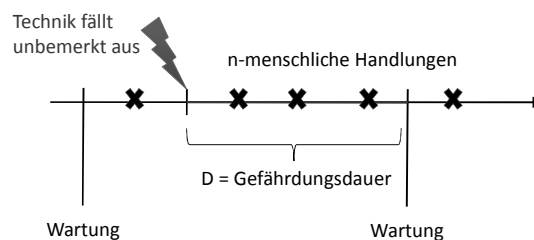


Abbildung 10-13 Risikomodell für PZB-Beispiel

Die menschlichen Handlungen, die durch die PZB überwacht werden, sind in der Regel Vorbeifahrten an einer H-Tafel (gekennzeichnet durch ein **x** auf der Zeitachse in Abbildung 10-13). Im Folgenden wird vereinfacht nur das Fahrzeuggerät der PZB betrachtet. Falls die PZB nun ausfällt, besteht für den Menschen keine Möglichkeit dies zu offenbaren, „da die PZB nur als verdeckt arbeitendes Überwachungssystem eingesetzt wird. Verdeckt bedeutet, dass der Tf von der PZB nur überwacht wird und keine Führungsgrößen, das heißt keine signaltechnische Information (Signalbegriffe, [...]), erhält“ (/98/).

Um die tolerierbare Versagenshäufigkeit für die technische Komponente berechnen zu können, ist die Frage zu beantworten, mit welcher Wahrscheinlichkeit der Mensch einen Fehler macht. Dabei ist zu beachten, dass dies nur dann gefährlich ist, wenn der menschliche Fehler stattfindet, nachdem die Technik ausgefallen ist und bevor die Gefährdung offenbart wird. Die Gefährdung kann in diesem Fall nur durch Wartung oder durch den eigentlichen Unfall offenbart werden (siehe auch Abbildung 10-13).

Die Überprüfung des Fahrzeuggeräts könnte beispielsweise erfolgen, wenn der Zug aus dem Depot fährt und durch eine Überfahrt eines scharfen Streckenmagneten getestet wird, ob der Fahrzeugmagnet noch funktioniert.

⁷⁰ Die Aufteilung kann möglicherweise besser durch ein Markov-Modell beschrieben werden. Hier wird jedoch weiterhin der Fehlerbaum genutzt, der in den vorigen Kapiteln schon eingesetzt wurde.

Für die Gefährungsdauer⁷¹ D wird im Rahmen dieses Rechenbeispiel der Mittelwert zwischen zwei Wartungen (bzw. Funktionstests) angenommen. Bei einem 16h Betriebstag, würde $D = 8h$ betragen, wenn die Wartung einmal pro Tag durchgeführt wird. Das ist ein beliebter Rechentrick, den man damit begründen kann, dass wenn ein Ausfall zufällig auftritt und das Zeitintervall zwischen zwei Tests T Zeiteinheiten lang ist, dann dauert es im Mittel $T/2$ Zeiteinheiten, bis der nächste Test den Ausfall offenbart. Die Wahrscheinlichkeit, dass die PZB zwischen zwei Wartungen ausfällt, berechnet sich aus $HR_{PZB} \cdot D$.

Die Wahrscheinlichkeit, dass der Mensch bei seinen n -Handlungen während einer Stunde einen Fehler macht, wird in der Regel mit der menschlichen Fehlerwahrscheinlichkeit für fertigungs-basierende Handlungen (unter normalen Umweltbedingungen) nach Hinzen angesetzt. Diese beträgt $Wk = 10^{-3}$. Es wird im Rahmen dieses Beispiels angenommen, dass der Zug ca. dreimal pro Stunde an einer H-Tafel vorbeifährt und der Mensch somit die Fahrgrenzen überwachen muss. Die Fehlerrate des Menschen beträgt dann näherungsweise $HR_{Mensch} = 3 \cdot 10^{-3}/h$. Die zulässige HR_{PZB} kann somit errechnet werden aus folgender Gleichung $THR_{Funktion} = HR_{Mensch} \cdot HR_{PZB} \cdot D$. Für das PZB-Fahrzeuggerät ergibt sich daraus eine $(T)HR_{PZB} = 1,25 \cdot 10^{-5}/h$ (siehe Abbildung 10-14).

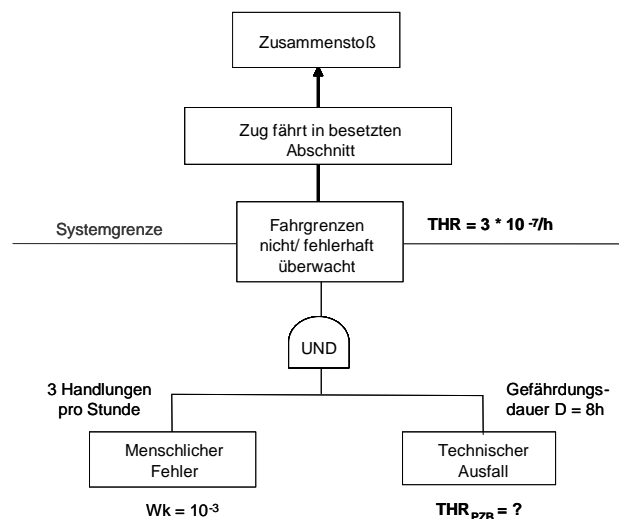


Abbildung 10-14 Beispiel für Aufteilung der THR

Nach /98/ sind mindestens die fahrzeugseitigen Anteile einer PZB (mit einem I60R Fahrzeuggerät) sicherheitsrelevante Funktionen im Sinne der EN 50129. Daraus kann geschlossen werden, dass diese Funktionen mindestens eine Gefährungsrate von $HR_{PZB} < 10^{-5}/h$ pro Funktion (/30/, Anhang A) besitzen, die somit die oben geforderte THR_{PZB} einhalten. Daraus kann geschlossen werden, dass bei Einsatz einer einfachen technischen Unterstützung, die im Regelfall schon heute auf ZLB-Strecken vorhanden ist, die oben abgeleiteten Anforderungen erfüllt werden können.

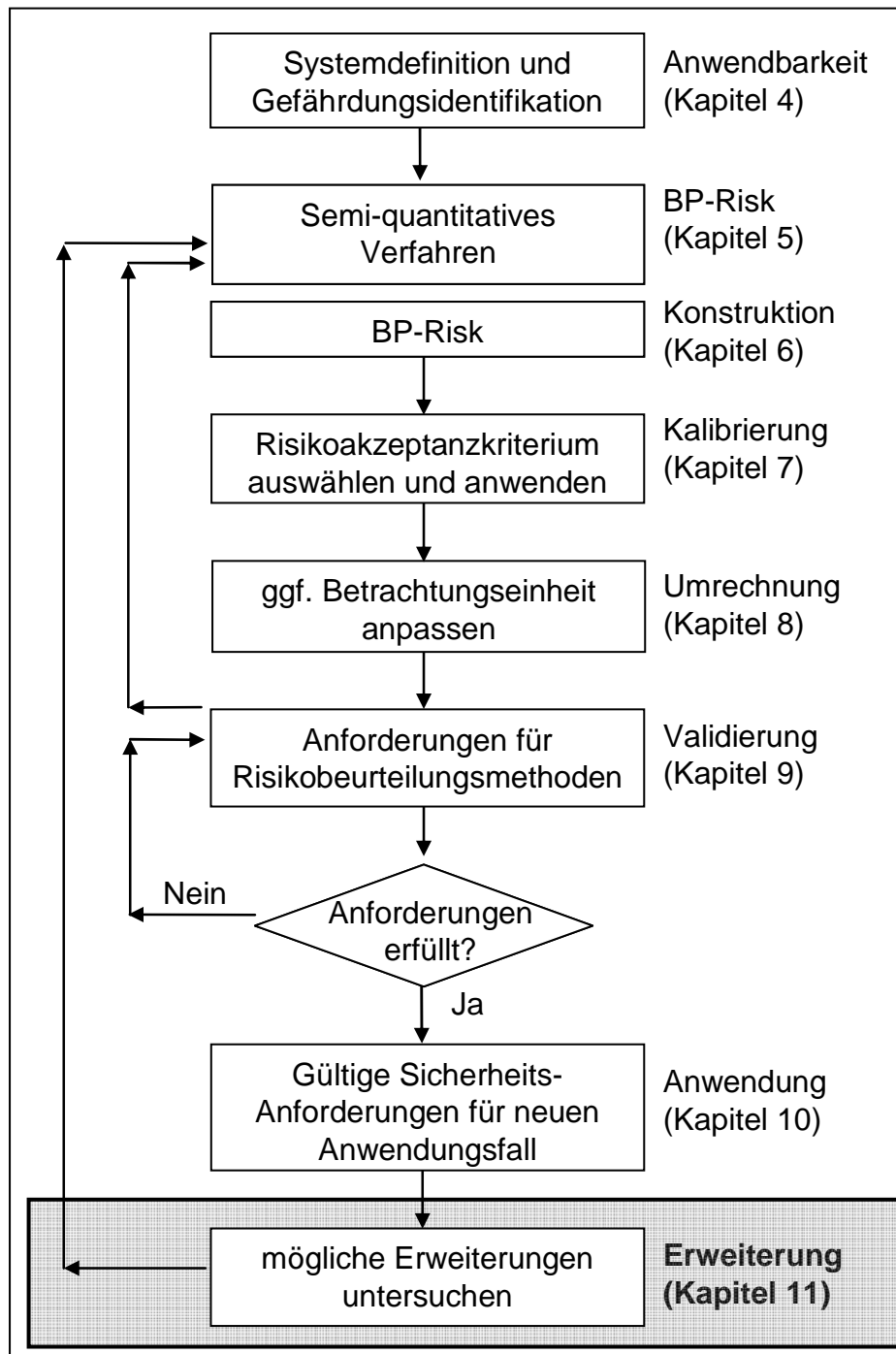
⁷¹ Die Gefährungsdauer spielt immer dann eine Rolle, wenn man Ausfälle, Fehler etc. nicht zeitnah aufdecken kann. Dann erhöht sich die Wahrscheinlichkeit proportional zur Zeit seit der letzten Offenbarung, Test etc. Macht man keine Ausfalloffenbarung, so strebt die Wahrscheinlichkeit gegen 1, d. h. der Beitrag zur Sicherheit ist vernachlässigbar.

Grundsätzlich ist zu beachten, dass die Entscheidung über das Betriebsverfahren in Deutschland alleinige Sache des Infrastrukturbetreibers ist. Dieser muss daher auch die technische Unterstützung für den Zugleitbetrieb realisieren. Somit kommen dafür hauptsächlich streckenseitige Komponenten in Frage. Würde diese technische Unterstützung Fahrzeugkomponenten erfordern, so müsste jedes Fahrzeug, das eine Zugleitstrecke befahren soll, über die entsprechende Ausrüstung verfügen. Bei Eingriff in die Fahrzeugsteuerung durch eine einfache Unterstützungstechnik muss die Zulassung des Fahrzeuges erweitert werden. In Deutschland werden daher heute für die technische Unterstützung des ZLB hauptsächlich infrastrukturseitige Komponenten angewendet, teilweise ergänzt um einen (elektronischen) Zugleiterarbeitsplatz. Das berücksichtigt auch die VDV-Schrift 752, indem sie den Streckenabschnittsschlüssel fordert (siehe Anhang G: VDV-Schrift 752). Im Ausland gibt es durch die fehlende rechtliche und organisatorische Trennung der Infrastruktur und des Verkehrs andere Techniken, die auch über Fahrzeuggeräte verfügen (/107/, Seite 91).

Das Wissen über die wahrscheinliche Realisierung der Funktionen auf der Strecke erfordert ggf. eine Anpassung der Bezugsgröße. So müsste für das hier genannte Beispiel einer PZB unterschieden werden zwischen den fahrzeug- und streckenseitigen Komponenten der punktförmigen Zugbeeinflussung. Für die streckenseitigen Komponenten wären beispielsweise die Wartungsintervalle sehr viel länger, so dass die Anforderung für die jeweilige Streckenkomponente höher werden würde. Da diese Entscheidung zur Designfreiheit des Anwenders gehört, wird an dieser Stelle nur auf die Beispiele aus Kapitel 8 verwiesen.

Bislang liegen im Rahmen der Risikobeurteilung mit BP-Risk die Anforderungen allgemein funktionsbezogen vor. Durch die generischen Funktionen und Gefährdungen sind möglicherweise in einigen Fällen die ungünstigeren Varianten angenommen worden, um auf der sicheren Seite zu bleiben. Dies wiederum führte möglicherweise zu etwas überhöhten Sicherheitsanforderungen, die im konkreten Fall noch abgestuft werden können, wenn detailliertere betriebliche Randbedingungen vorliegen. Durch die Einführung von Subszenarien wurde versucht, den worst-case Annahmen entgegenzuwirken, indem die Randbedingungen der Gefährdungen konkretisiert wurden.

Zusammenfassend kann gesagt werden, dass die Risikobeurteilung mit Hilfe von BP-Risk einen entscheidenden Zeit- und damit Kostengewinn mit sich bringt. BP-Risk ist als Methode für diesen Anwendungsfall besonders gut geeignet, da es ein System von Mensch und Technik bewertet so dass dort keine gesonderten Betrachtungen in Form von Ereignis- oder Fehlerbäumen für menschliche Handlungen nötig waren. Dies war oft in vergangenen Risikoanalysen der Fall. Durch die Vorgaben der Funktionsliste und der Analyseebene sowie die bereits erfolgte Einarbeitung des Risikoakzeptanzkriteriums nimmt BP-Risk dem Anwender ebenfalls viel Arbeit ab. Die eigentliche Anwendung der BP-Risk-Tabellen ist sehr einfach und handlich. Dem Anwender bleiben natürlich die Begründung und die Dokumentation der Ergebnisse. Es muss dem Anwender außerdem bewusst sein, dass eine Methode, wie BP-Risk (aber auch jede andere Methode zur Risikoanalyse) ihm nicht das selbstständige Denken und das ausreichende Verständnis über das zu bewertende System abnehmen kann.



11 Erweiterung

BP-Risk basiert auf einem generischen Risikomodell. In Rahmen dieser Arbeit fand die Projektierung dieser Methodik vor allem für die Leit- und Sicherungstechnik statt. Das Grundmodell kann jedoch durch Anpassung der Parameter auch für andere Bereiche angewendet werden. Dieses geschah bereits für ein völlig anderes Anwendungsfeld, nämlich der Kraftwerkstechnik im Bereich der Siemens Power Generation (PG). Dort wurde BP-Risk fachspezifisch abgewandelt und ist für die Ableitung von Sicherheitsanforderungen für Funktionen im Turbinenbau vom TÜV zugelassen worden. Die Parameter von BP-Risk konnten für diesen Anwendungsbereich aufwandsarm angepasst werden und die Methode wurde entsprechend kalibriert. Sie wird mittlerweile als Standardmethode unter dem Namen PG-Risk eingesetzt. Über die Anwendung für funktionale Sicherheit im Bereich Maschinensicherheit oder Medizin wird innerhalb der Siemens AG diskutiert. Naheliegender wäre auch eine Anpassung für den Bereich Fahrzeuge (TR – Trains). Dazu wurden bereits erste interne Untersuchungen durchgeführt (nicht veröffentlicht).

In Kapitel 6.2.3 wurde im Rahmen der Bewertung von Personenschäden bereits darauf hingewiesen, dass für den Parameter *A* der Unfalltyp *‚Gefährliches Ereignis mit Reisenden‘* und auch die Besetzung der Züge nicht berücksichtigt wurden. Im Folgenden werden für diese beiden Aspekte – Reisendensicherung und Zugbesetzung – mögliche Erweiterungen für BP-Risk kurz vorgestellt. Es ist zu beachten, dass die folgenden Ausführungen keine abschließenden Ergebnisse präsentieren, sondern lediglich Vorschläge und Ideen liefern, die ggf. weiterentwickelt werden können.

11.1 Gefährliche Ereignisse mit Reisenden

Zurzeit beschränkt sich BP-Risk auf gefährliche Ereignisse, die einen Zug betreffen. Es werden also Unfälle betrachtet, bei dem der Zug beschädigt wird. Wünschenswert wäre es, wenn sich der Ansatz auf Personensicherheit erweitern ließe, d. h. auch diejenigen Unfälle betrachtet werden, bei denen Personen beschädigt werden, der Zug jedoch *‚heil‘* bleibt. Es handelt sich hierbei also um ein anderes Risikomodell.

Die EBA-Anweisung A21 definiert *‚Gefährliches Ereignis mit Reisenden‘* als *‚jedes Ereignis, bei dem Reisende konkret gefährdet oder geschädigt werden‘* (/56/). Hierbei sind Suizide und Arbeitsunfälle ausgeschlossen. Die *‚Zusätzliche Feststellung‘* (Anhang der EBA-Anweisung 21) unterscheidet dabei folgende Fälle:

- Ereignis, verursacht durch Infrastrukturmangel,
- Einsteigeunfall,
- Aussteigeunfall, und
- Sturz aus dem fahrenden Zug.

Beim Ereignis, verursacht durch Infrastrukturmangel wird der Ort des Ereignisses berücksichtigt (z. B. Bahnhofshalle, Unterführung, Bahnsteigzugang, Treppe oder Aufzug zum Bahnsteig, usw.), sowie der Bodenbelag und ob Gedränge herrscht. Bei den anderen drei Ereignissen wird unterschieden, wo sich der Zug befindet (Bahnsteig, freie Strecke, Gleiskrümmung, Geraden) und wie der Abfahrtsvorgang abläuft (Standort des Personals, Zuständigkeiten usw.). Bei Ein- oder Aussteigeunfällen werden sowohl Gedränge und Überfüllung als auch die geschätzte Geschwindigkeit (unter oder über 5 km/h) berücksichtigt. Es werden außerdem Aussagen zur Wagenausrüstung und Türsicherung gemacht. Diese Angaben aus der EBA-Anweisung können erste Hinweise geben, was zur Bewertung der Reisendensicherung berücksichtigt werden sollte.

Bei der RPN-Methode, die auf dem gleichen Ansatz wie BP-Risk beruht, wird die Reisendensicherung bereits durch Einführung eines zusätzlichen Parameters berücksichtigt. Es wird versucht, diese Idee für BP-Risk zu übernehmen und anzupassen.

Normalerweise ergibt sich die Ermittlung des Parameters Schadensausmaß S bei Zugunfällen aus der Bewertung der drei Subparameter,

- Zuggattung (T),
- Maßgebliche Geschwindigkeit (V), und
- Anzahl betroffener Personen (A),

welche addiert den Parameterwert S ergeben: $S = T + V + A$. Grundlage dabei ist die kinetische Energie, da es sich um einen Zug in Bewegung (also eine bewegende Masse) handelt.

Die Ermittlung des Parameters ‚Schadensausmaß‘ ergäbe sich in Anlehnung an die RPN-Methode bei ‚Gefährlichen Ereignissen mit Reisenden‘ nur aus der Bewertung des neuen Subparameters A^* . Die Geschwindigkeit würde in diesem Fall zu Null gesetzt ($V = 0$) werden, da die maßgebliche Geschwindigkeit laut EBA-Anweisung ca. 5 km/h beträgt und somit vernachlässigt werden kann. Zum Vergleich liegt der quantitative Wert für geringe Geschwindigkeiten im Rahmen von BP-Risk bei ca. 38 km/h.

Die Zuggattung würde auch keine Rolle spielen, da die kinetische Energie nicht berücksichtigt wird und somit auch die Masse des Zuges keine Relevanz mehr hat ($T = 0$).

Auch die Betriebsdichte im Rahmen der Gefahrenabwehr kann für den Unfalltyp ‚Gefährliches Ereignis mit Reisenden‘ vernachlässigt werden ($B = 0$), da die Besetzung des nächsten Abschnittes für ein solches Gefährdungsszenario keine Rolle spielt. Denkbare Szenarien von Personenunfällen wären eher (siehe auch /84/):

- Türöffnung während der Fahrt,
- Unangemessene Zwangsbremmung,
- Unzeitige Türöffnung am Bahnsteig,
- Zug rollt während des Ein- und Aussteigens an,
- Zur Unzeit schließende Tür (bei Zugstillstand),
- Person verletzt sich im Zug.

Um eine quantitative Grundlage für den neuen Parameter A^* zu erhalten, werden deutsche und europäische Statistiken herangezogen.

Der ursprüngliche Parameter A wurde mit Hilfe einer DB-Unfallstatistik aufgestellt, die im Rahmen der Risikoanalyse FFB (/109/) verwendet wurde. Diese Statistik enthält den Unfalltyp ‚Gefährliche Ereignisse mit Reisenden‘ nicht explizit, jedoch zumindest eine Art Teilmenge davon, nämlich die Kategorie ‚Personenunfälle‘. In dieser Kategorie fanden an höhengleichen Bahnsteigzugängen nur 9 Unfälle in 10 Jahren (von 1989 – 1999) statt. Der Wert nach der bekannten Heuristik aus Kapitel 6.2.3 beträgt ca. 0,5 Personenschaden je Unfall, wobei nur die Personengruppen Reisende und Mitarbeiter betrachtet wurden. Im Vergleich dazu beträgt nach Tabelle 6-10 der höchste Wert für den Unfalltyp Zusammenstoß 0,157 Personenschaden je Unfall für Reisende und Mitarbeiter, also nur ein Drittel davon. Da die Gewichtung der Personenschäden für die Kategorie ‚Personenunfälle‘ im Vergleich zu den Zugunfällen viel zu stark ist, kann dieser Wert erst einmal nicht pauschal in der Tabelle für den ursprünglichen Parameter A berücksichtigt werden.

Alternativ werden die Statistiken des Statistischen Amtes der Europäischen Gemeinschaften (EUROSTAT) herangezogen. Die EUROSTAT stellt Statistiken für die Länder der EU zusammen, die von den nationalen statistischen Ämtern der Mitgliedstaaten erhoben und zur Verfügung gestellt werden. Die Daten sind in einer öffentlichen Datenbank im Internet abrufbar. Für die Kategorie ‚Unfälle im Eisenbahnverkehr‘ kann die jährliche Zahl der Opfer je Unfallart abgefragt werden. Abbildung 11-1 zeigt die jährlichen Opfer für die Kategorie ‚Personenunfälle durch sich bewegendes rollendes Material‘ in Deutschland in den Jahren 2004 und 2005⁷².

| | | | |
|--|--|-------------|------------------------|
| unit | nbr Anzahl/Absoluter Wert/Einheit | | |
| geo | de Deutschland (einschließlich ex-DDR seit 1991) | | |
| originac | acc_pers Personenunfälle durch sich bewegendes rollendes Material | | |
| | | time | 2004a00 2005a00 |
| pers_acc | victim | | |
| pass_tot Fahrgäste - Insgesamt | kil Tote | 7 | 6 |
| | inj Verletzte | 10 | 32 |
| rail_empl Eisenbahnbeschäftigte | kil Tote | 5 | 6 |
| | inj Verletzte | 27 | 24 |
| oth Sonstige | kil Tote | 88 | 94 |
| | inj Verletzte | 69 | 40 |

Abbildung 11-1 Opfer bei Personenunfällen nach EUROSTAT (/64/)

⁷² Viele Daten sind in EUROSTAT erst ab dem Jahr 2004 eingetragen.

Die Statistik aus Abbildung 11-1 besagt, dass in den Jahren 2004 und 2005 insgesamt 13 getötete und 42 verletzte Fahrgäste sowie 11 getötete und 51 verletzte Eisenbahnbeschäftigte in dieser Kategorie betroffen waren. Dritte (Sonstige) werden hier vorerst nicht betrachtet. Die in Kapitel 6.2.3 eingeführte Formel wird zur Berechnung der äquivalenten Personenschäden angewendet, wobei hier ein Mittelwert für Schwer- und Leichtverletzte ermittelt wird, da in der Statistik diese nicht unterschieden werden:

Personenschaden = $13 + 11 + (42 + 51)/50 = 25,86$ (in den Jahren 2004 und 2005).

Anhand der Statistik über die Anzahl der Personenunfälle aus Abbildung 11-2 kann der äquivalente Personenschaden pro Unfall ermittelt werden zu:

$25,86 / (294 + 296) = 0,0438$ Personenschaden pro Unfall

| | | |
|---|----------------------|------|
| geo de Deutschland (einschließlich ex-DDR seit 1991) | | |
| unit nbr Anzahl/Absoluter Wert/Einheit | | |
| | time 2004a00 2005a00 | |
| originac | | |
| total Insgesamt | 1172 | 1111 |
| acc_pers Personenunfälle durch sich bewegendes rollendes Material | 294 | 296 |

Abbildung 11-2 Anzahl der Personenunfälle nach EUROSTAT (/64/)

Dieser Wert würde sich in Tabelle 6-10 für Parameter A zwischen einer Entgleisung (0,014 Personenschaden pro Unfall) und einem Zusammenstoß (0,157 Personenschaden pro Unfall) wiederfinden, was einer realistischeren Einstufung entspräche als der aus der DB-Statistik.

Die DB-Statistik betrachtet zwar einen Zeitraum von 10 Jahren und sollte somit einen zuverlässigeren Wert liefern, allerdings wird nur ein Teil der Kategorie ‚Gefährliche Ereignisse mit Reisenden‘ berücksichtigt. Und selbst für einen Teilbereich ist der Wert eigentlich schon zu hoch, wobei beachtet werden müsste, dass die Parameter V und T nicht zum Schadensausmaß beitragen und außerdem die Gefahrenabwehr nur noch den menschlichen Nothandlungen abhinge ($B = 0$).

Die EUROSTAT Statistik berücksichtigt lediglich einen Zeitraum von zwei Jahren, passt jedoch vom Wert her besser in die Tabelle des ursprünglichen Parameter A. Es bedarf weiterer statistischer Untersuchungen, um geeignete Daten für die Kategorie ‚Gefährliches Ereignis mit Reisenden‘ zu sammeln und ggf. das Risikomodell von BP-Risk zu erweitern. Zu klären bleibt grundsätzlich, ob die beiden unterschiedlichen Risikomodelle ineinander überführbar sind.

11.2 Besetzung der Züge

In Kapitel 6.2.3 wurde bereits darauf hingewiesen, dass im Rahmen des Parameters *A* nicht die Besetzung der Züge berücksichtigt wird. Dieser Aspekt wäre jedoch interessant, da beispielsweise Personenzüge sehr viele Personen an Bord haben können und Güterzüge möglicherweise nur den Triebfahrzeugführer (Tf). Die Besetzung der Züge ist außerdem unterschiedlich im Nah- und Fernverkehr und auch zu bestimmten Tages- und Jahreszeiten. Beispielhaft zeigt Tabelle 11-1 die durchschnittliche Besetzung (Anzahl von Personen) in Abhängigkeit der Zuggattung.

Tabelle 11-1 Durchschnittliche Besetzung der Züge (nach /1/)

| Zuggattung (alt) | Zuggattung (neu) | Durchschnittliche Besetzung [Personen] |
|--------------------|-----------------------|--|
| IC (Inter City) | IC (Inter City) | 360 |
| D (Schnellzug) | IR (Inter Regio) | 390 |
| E (Eilzug) | RE (Regional Express) | 300 |
| N (Nahverkehrszug) | RB (Regional Bahn) | 210 |

Es bleibt zu klären, inwiefern diese Daten im Rahmen des Parameters *A* mitberücksichtigt werden können, da dieser ja bereits zwei Aspekte – Personenschäden und Unfalltyp vereint. Es ist anzunehmen, dass es schwierig wäre, noch einen dritten Aspekt einfließen zu lassen.

Da es bereits einen Parameter zur Berücksichtigung der Masse in Abhängigkeit der Zuggattung gibt (Parameter *T*), wäre es vielleicht möglich, die Besetzung der Züge über den Parameter *T* mit einfließen zu lassen. Dies wiederum würde jedoch den Parameter *T* etwas unübersichtlich machen, da zwischen Masse und Besetzung der Züge erst einmal kein Zusammenhang besteht. Ein eigenständiger Parameter zur Besetzung der Züge würde aus Sicht der Verfasserin jedoch auch keinen Sinn haben, da die Logarithmierung der Werte aus Tabelle 11-1 keine signifikanten Unterschiede ergeben, so dass eine Klassifizierung nicht möglich ist – zumindest nicht, wenn die Basis Wurzel 10 zugrunde gelegt wird (siehe Tabelle 11-2).

Tabelle 11-2 Logarithmus für die Besetzung der Züge

| Besetzung | Log (Basis Wurzel 10) |
|-----------|-----------------------|
| 390 | 5,18 |
| 360 | 5,11 |
| 300 | 4,95 |
| 210 | 4,64 |

Insofern sind entweder andere Daten (möglicherweise mit einem anderen Bezug) zur Berücksichtigung der Personenbesetzung in den Zügen notwendig oder eine sinnvolle (mathematische) Berücksichtigung dieses Aspektes im Rahmen des Parameters *T*.

12 Schlussfolgerung

Im Rahmen einer Risikobeurteilung wird ein System untersucht, um Gefährdungen und Schwachstellen aufzuzeigen. Bei der Suche nach möglichen Gefahren wird das System detailliert betrachtet, wobei sich das Verständnis für das System verbessert. Dadurch wird es möglich, Anforderungen an Betrieb und Konstruktion festzulegen, die den sicheren Betrieb gewährleisten. Außerdem kann man aus der vertieften Kenntnis der Gefährdungen Maßnahmen ableiten, mit denen das Risiko beherrscht werden kann.

Die in den vorangegangenen Kapiteln vorgestellte Methode zur Risikobeurteilung BP-Risk ermöglicht es, Sicherheitsanforderungen in der Eisenbahntechnik praktikabel und kostengünstig abzuleiten.

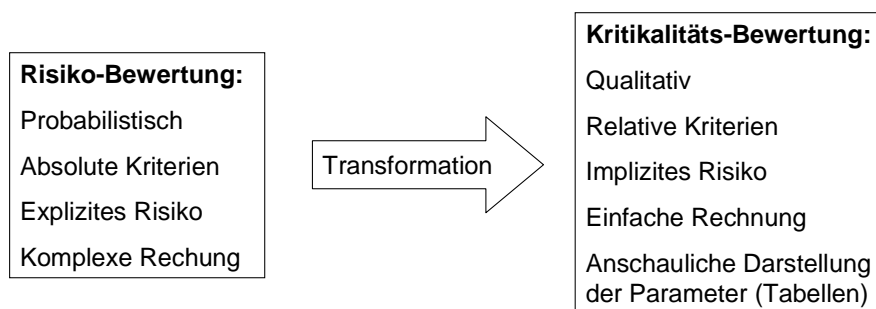


Abbildung 12-1 Risiko- und Kritikalitätsbewertung

Der BP-Risk Ansatz ist eine einfach anzuwendende Methode zur Risikobeurteilung, die auf einem verbesserten Risikoprioritätszahlen-Konzept beruht. Der Ansatz basiert auf einem soliden Modell mit einer angemessenen mathematischen Aufbereitung und einer ingenieurmäßigen Konstruktion der einzelnen Tabellen für die Subparameter (siehe Abbildung 12-1). Die Vorteile der Konstruktion von BP-Risk sind, dass alle relevanten Parameter abgebildet und präzise beschrieben werden, indem sie mit konkreten Zahlenwerten hinterlegt sind. Die Einzelparameter sind in leicht zu schätzende Teilparameter verfeinert. Die Konstruktion ist nachvollziehbar skaliert; dadurch sind ihre Ergebnisse nachhaltig vergleichbar. Die solide Konstruktion wird bei der anwenderfreundlichen Gestaltung der Methode beibehalten. Die Offenlegung aller Annahmen, Modelle und Bewertungskriterien sowie Anforderungen ermöglicht als wissenschaftliches Prinzip auch eine denkbare Widerlegung des Modells.

Ein weiterer Vorteil von BP-Risk ist insofern erwähnenswert, da zurzeit die Diskussion über kleine betriebliche Änderungen sehr aktuell ist. Da BP-Risk qualitative Beschreibungen für die einzelnen Parameterklassen verwendet und diese somit eine konstruierte Genauigkeit haben, bleiben beispielsweise kleine Geschwindigkeitsänderungen oder eine geringe Erhöhung der Taktfolge in der derselben Klasse. Somit erfüllt BP-Risk auch die ERA-Anforderung für explizite Risikoeinschätzungen, die besagt, „dass geringfügige Änderungen bei zu Grunde gelegten Annahmen oder Voraussetzungen nicht zu erheblichen Unterschieden bei den Anforderungen führen“ (/59/, Artikel 10) sollen.

Neben den objektiv nachweisbaren Eigenschaften gibt es aber noch eine Reihe qualitativer Vorteile:

- Im Vergleich zu quantitativen Methoden ist BP-Risk wesentlich effizienter. Zwar wird nur ein Teil der Risikobeurteilung vereinfacht, aber es steht nach /9/ (Seite 109) zu erwarten, dass bis zu 40% des Aufwands im Vergleich zu quantitativen Risikobeurteilungen reduziert wird. Die Ergebnisse aus der Anwendung für ZLB haben gezeigt, dass die System- und die Gefährdungsidentifikation immer noch sehr viel Zeit in Anspruch nehmen, wobei schon Hilfsmittel in Form der Funktionsliste zur Verfügung stehen. Die eigentliche Anwendung der BP-Risk-Tabellen ist hingegen sehr einfach und schnell.
- Der Vergleich der Effizienz mit angloamerikanischen Ansätzen fällt noch wesentlich besser aus, da BP-Risk generische und damit streckenunabhängige Risikobeurteilungen zulässt.
- Gegenüber anderen quantitativen Methoden besteht neben der soliden Konstruktion ein weiterer Vorteil darin, dass BP-Risk nicht aufwändiger als andere Verfahren ist, aber dass alle wesentlichen Parameter der Risikoformel abgebildet werden und dass die Parameter wesentlich besser beschrieben sind. Dies wird insbesondere am Beispiel des Schadensausmaßes deutlich, wo BP-Risk statt eines einzigen Parameters eine wesentlich verlässlichere Einschätzung mit drei Teilparametern bietet.
- Aufgrund der nachvollziehbaren, rigorosen Konstruktion konnten in Reviews mit Fachexperten bisher keine Gründe erkannt werden, die einer Verwendung als Methode zur Risikobeurteilung in der Eisenbahn-Automatisierungstechnik im Wege stehen. Dies wurde auch vom Eisenbahnbundesamt bestätigt. *„Das Eisenbahn-Bundesamt (EBA) hat die generelle Eignung [von BP-Risk] für Risikoanalysen in der Eisenbahntechnik und die Konformität zu den dort geltenden CENELEC-Normen bestätigt“ (/15/ und /18/).*
- Das BP-Risk Verfahren wurde bereits erfolgreich in anderen Industriesektoren angewendet (PG-Risk). Eine Erweiterung von BP-Risk zur Betrachtung der Reisendensicherung und Besetzung der Züge ist denkbar.
- BP-Risk besitzt das Potential zu einer einheitlichen Methode für die gesamte Eisenbahntechnik, ggf. mit Anpassungen für unterschiedliche Gewerke. Eine solche einheitliche Vorgehensweise wäre ein unschätzbarer Vorteil, mit dem nicht einmal die Luftfahrt aufwarten kann.

13 Zusammenfassung und Ausblick

Zusammenfassend ist festzustellen, dass der dargelegte wissenschaftliche Fortschritt in folgenden Aspekten besteht:

BP-Risk hat eine standardisierte Systemdefinition. Durch die Vorgabe einer Funktionsliste, die bald in einer europäischen Norm gültig sein wird, konnte eine fundierte und anwenderfreundliche Systemdefinition erarbeitet werden. Zusätzliche Funktionen wurden durch eine Erweiterung der Funktionsliste auf der betrachteten Ebene eingeführt.

BP-Risk wurde für neue Anforderungen angepasst. Im Vergleich zur veröffentlichten Version wurden Parameter angepasst und das Verfahren optimiert, z. B. durch die Einschränkung der Bandbreite des Schadensparameters.

BP-Risk ist europäisch kalibriert. Die bereits veröffentlichte Version war lediglich anhand nationaler Risikoanalysen kalibriert worden. Mit der Implementierung eines europäischen Risikoakzeptanzkriteriums, was sogar die zukünftige europäische Gesetzgebung erfüllt, ist BP-Risk nun europaweit einsetzbar.

BP-Risk ist validiert. Es wurde gezeigt, dass BP-Risk die europäischen Anforderungen für Common Safety Methods und explizite Risikoanalysen erfüllt.

BP-Risk wurde auf ein neues Anwendungsbeispiel angewendet. Für den Zugleitbetrieb konnten mit Hilfe von BP-Risk gültige Sicherheitsanforderungen schnell und praktikabel abgeleitet werden, wobei der neue CSM-Prozess der ERA zum ersten Mal an einem praktischen Beispiel eingesetzt wurde.

BP-Risk ist zurzeit der einzige qualitative Ansatz, für den eine strenge Begründung vorliegt, welche im Rahmen dieser Arbeit nachvollziehbar aufgezeigt wurde. *„Dieses Verfahren ist weltweit das einzige, für das Korrektheit nachgewiesen wurde. Es darf sich zu Recht semi-quantitativ nennen, da es eine qualitative Vorgehensweise mit einer ingenieurwissenschaftlichen Konstruktion verbindet“* (/17/).

Aus Sicht der Verfasserin werden qualitative und semi-quantitative Methoden zukünftig aufgrund ihrer bereits genannten Vorteile eine wichtige Rolle im Rahmen der Common Safety Methods spielen. Als semi-quantitativer Ansatz hat BP-Risk das Potential, eine der ersten begründeten und praktikablen Methoden zu werden, die als explizite Risikoeinschätzung die ERA-Anforderungen erfüllt. Außerdem ist BP-Risk nicht auf die Eisenbahnsignaltechnik beschränkt. Die Anpassung an einen anderen speziellen Anwendungsbereich wurde bereits für Siemens Power Generation erfolgreich durchgeführt. Mit BP-Risk verbindet sich die Hoffnung der Forscher und Entwickler, dass sie eine effiziente Standardmethode für Risikoanalysen wird.

ANHANG

| | |
|--|------------|
| Anhang A: Terminologie | 183 |
| Anhang B: Abkürzungsverzeichnis | 187 |
| Anhang C: TSI..... | 192 |
| Anhang D: Streckenstandards | 193 |
| Anhang E: Funktionsliste | 194 |
| Anhang F: Berechnung BÜ..... | 206 |
| Anhang G: VDV-Schrift 752 | 207 |
| Anhang H: Funktionen ZLB | 208 |
| Literaturverzeichnis | 209 |

Anhang A: Terminologie

Es wird die in der internationalen Normung übliche Terminologie verwendet (siehe hierzu IEC 60300-3-9 (Entwurf) (/78/), IEC 61226:2005 (/75/), IEC 61508 (/74/), ISO/IEC Guide 51 (/79/), ISO/IEC Guide 73 (Entwurf) (/80/), EN 50126 (/28/), EN 50129 (/30/), prEN0015380-4:2007 (/32/), Direktive 2004/49/EC (/48/), EG-Verordnung 91/2003 (/50/)).

Im Folgenden werden die wichtigsten Begriffe kurz wiedergegeben.

Anerkannte Regeln der Technik: ein schriftlich niedergelegtes Regelpaket, das bei ordnungsgemäßer Anwendung zum Ausschluss einer oder mehrerer spezieller Gefährdungen zur Anwendung gelangen kann.

Anforderung: erforderliche Bedingung oder Fähigkeit, um die Lösungen einer Aufgabe oder eines Zwecks zu beschränken.

Ausfall (Versagen): Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen.

Common Safety Target: Sicherheitsniveau, das von verschiedenen Teilen des Eisenbahnsystems mindestens erreicht werden muss, ausgedrückt durch ein Risikoakzeptanzkriterium.

Common Safety Method: zu entwickelnde Methode, die beschreibt, wie das Sicherheitsniveau und das Erreichen der Sicherheitsziele sowie die Erfüllung von anderen Sicherheitsanforderungen, festgestellt werden.

Eisenbahnsystem: System, das durch die Strecken und ortsfeste Anlagen umfassenden Eisenbahninfrastrukturen des vorhandenen Eisenbahnnetzes und durch die auf diesen Infrastrukturen verkehrenden Fahrzeuge sowie durch die bestehenden Betriebsvorschriften gebildet wird.

Entgleisung: das Abgleiten oder Abheben eines Eisenbahnfahrzeugs von der Fahrbahn, auch wenn es sich selbst wieder aufgleist, oder der zweisepurige Lauf eines Eisenbahnfahrzeugs (EBA Definition).

Ereignis: Auftreten einer bestimmten Reihe von Umständen.

Fahrgast (Reisender): eine mit der Eisenbahn reisende Person mit Ausnahme des Zugpersonals⁷³. Nutzer von Eisenbahnfahrzeugen oder Bahnsteiganlagen – einschließlich Zu- und Abgängen, ausgenommen Mitarbeiter der Eisenbahnunternehmen im Dienst.

⁷³ Für Zwecke der Unfallstatistik sind die Fahrgäste eingeschlossen, die versuchen, auf einen fahrenden Zug aufzuspringen oder von einem fahrenden Zug abzuspringen.

Fehler: Verminderung oder Verlust der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen.

Folge: Resultat eines Ereignisses, das eine Auswirkung auf die Sicherheit hat.

Funktion: bestimmter Zweck oder zu erreichendes Ziel, der oder das spezifiziert oder näher beschrieben werden kann, ohne Bezug auf die physikalischen Mittel zu nehmen.

Funktionale Anforderung: formuliert die Anforderungen für eine bestimmte Funktion.

Funktionale Sicherheit: ist der Teil der Sicherheit eines Systems, der von der korrekten Funktion der sicherheitsbezogenen (Sub-)Systeme und externer Einrichtungen zur Risikominderung abhängt.

Gefährdung: Bedingung, die zu einem Unfall führen kann.

Gefährliches Ereignis mit Reisenden: jedes Ereignis, bei dem Reisende konkret gefährdet oder geschädigt werden (EBA Definition).

Getötete: alle Personen, die entweder unmittelbar nach einem Unfall oder innerhalb von 30 Tagen an den Unfallfolgen sterben – mit Ausnahme der Personen, die Selbstmord begangen haben.

Kollision mit Hindernissen (Aufprall auf Hindernisse): das Fahren gegen ein Hindernis im Regellichtraum, nicht aber gegen ein anderes Eisenbahnfahrzeug. Der Arbeitsunfall bleibt hiervon unberührt (EBA Definition).

Kollision von Zügen (Zusammenstoß): das Auffahren eines Eisenbahnfahrzeugs auf ein anderes Eisenbahnfahrzeug (EBA Definition).

Menschliches Versagen: Handlung oder Unterlassung eines Menschen, die zu einem unerwünschten Ergebnis führen.

Restrisiko: verbleibendes Risiko nach Realisierung der Sicherheitsmaßnahmen.

Risiko: Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.

Risikoanalyse (engl.: risk analysis): Vorgang, bei dem in systematischer Weise anhand vorliegender Information Gefährdungen identifiziert und das Risiko für eine einzelne Person, für Personengruppen, für Sachen oder für die Umwelt eingeschätzt werden.

Risikoakzeptanzkriterien: Bezugskriterien, auf deren Grundlage die Vertretbarkeit eines Risikos bewertet wird.

Risikobeurteilung (engl.: risk assessment): gesamter Vorgang aus Risikoidentifizierung, -analyse und -bewertung.

Risikobewertung (engl.: risk evaluation): Vorgang der Abwägung zur Vertretbarkeit eines Risikos auf Grundlage der Risikoanalysen und unter Einbeziehung von Faktoren wie sozioökonomischer und umweltbezogener Einflussgrößen.

Risikoeinschätzung (engl.: risk estimation): Verfahren, um den Wahrscheinlichkeiten und den Folgen des Risikos Werte zuzuordnen.

Risikomanagement: systematische Anwendung von Managementgrundsätzen, -verfahren und -praktiken zur Analyse, Bewertung und Steuerung/Bewältigung von Risiken.

Risikoreduktion: Maßnahmen, um die zum Risiko zugehörige Wahrscheinlichkeit, dessen Ausmaß oder beides zu vermindern.

Schaden: Physische Verletzung oder Schädigung der Gesundheit von Menschen, entweder direkt oder indirekt als ein Ergebnis von Schäden von Gütern oder der Umwelt.

Schwerverletzte: alle Verletzten, die nach einem Unfall für mehr als 24 Stunden in ein Krankenhaus eingewiesen wurden, mit Ausnahme der Personen, die einen Selbstmordversuch unternommen haben. Personen, die als Folge der durch einen Eisenbahnunfall erlittenen Verletzungen für mehr als drei Tage arbeitsunfähig sind.

Sicherheit: Freiheit von unvertretbaren Risiken („Schutz vor unbeabsichtigten Schäden“).

Sicherung: Verhinderung von nicht autorisierten Zugriffen zu Anlagen, Einrichtungen und Daten („Schutz vor böswilligen Schäden“).

Sicherheitsanforderungen: bezeichnet die (qualitativen oder quantitativen) Sicherheitsmerkmale eines Systems und seines Betriebs (einschließlich Betriebsvorschriften), die zur Erfüllung beispielsweise gesetzlicher oder unternehmensspezifischer Sicherheitsziele erforderlich sind.

Sicherheitsintegrität: Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraums anforderungsgemäß ausführt.

System: Festumrissene Menge von Elementen, die nach einem Plan in gegenseitiger Beziehung stehen. Ein Element eines Systems kann zugleich ein anderes System sein (genannt Teilsystem).

Tolerierbares Risiko: Risiko, das - basierend auf den aktuellen gesellschaftlichen Wertvorstellungen - in einem gegebenen Zusammenhang tragbar ist.

Unfall: ein nicht beabsichtigtes Ereignis oder eine Reihe von Ereignissen mit der Folge von Toten, von Verletzten, des Verlustes eines Systems oder von Umweltschäden.

Unfall am Bahnübergang (Zusammenprall): das Zusammentreffen von einem Eisenbahnfahrzeug und einem Straßenverkehrsteilnehmer auf einem Bahnübergang (EBA Definition).

Unfall mit Personen (Aufprall auf Personen): das Fahren gegen Personen (nicht: Reisende) im Regellichraum. Der Arbeitsunfall bleibt hiervon unberührt (EBA Definition).

Ursache: zugrunde liegender interner oder externer Faktor, der zu einem Ereignis führt.

Validierung: Bestätigung durch Überprüfung und objektiven Nachweis, dass die besonderen Anforderungen für einen spezifischen, bestimmungsgemäßen Gebrauch erfüllt wurden.

Zug: ein oder mehrere Eisenbahnfahrzeuge, das/die von einer oder mehreren Lokomotiven bzw. Schienenfahrzeugen gezogen wird/werden, oder ein allein fahrendes Eisenbahnfahrzeug, das unter einer bestimmten Nummer oder einer besonderen Bezeichnung von einem festen Ausgangspunkt zu einem festen Endpunkt fährt. Leerlokomotiven (allein verkehrende Loks) gelten nicht als Zug.

Anhang B: Abkürzungsverzeichnis

A

| | |
|----------------|--|
| a (A) | Anzahl betroffener Personen (in BP-Risk) |
| A _k | Accident (Unfall - in der Risikoformel) |
| ABS | Ausbaustrecke |
| AEG | Allgemeines Eisenbahngesetz |
| AEIF | Association Européenne pour l'Interopérabilité Ferroviaire (Europäische Vereinigung für die Interoperabilität im Bereich der Bahn) |
| Ak | Ankunftsmeldung (Zuglaufmeldung beim Zugleitbetrieb) |
| ALARP | As Low As Reasonable Practical (britisches Risikoakzeptanzkriterium) |
| ARP | Aerospace Recommended Practice (von den Luftbehörden herausgegebene Sammlung von Dokumenten, welche die Anforderungen an komplexe Systeme in Flugzeugen beschreiben) |
| As | Abstellmeldung (Zuglaufmeldung beim Zugleitbetrieb) |
| ASCAP | Axiomatic Safety-Critical Assessment Process (quantitative Methode zur Risikobeurteilung) |
| ASIL | automobilspezifischer SIL |
| ATP | Automatic Train Protection (Automatische Zugbeeinflussung) |

B

| | |
|----------|--|
| b (B) | betriebliche Randbedingungen (in BP-Risk) |
| BfV | Bundesministerium für Verkehr |
| BO-Strab | Verordnung für den Bau und Betrieb der Straßenbahnen |
| BP-Risk | Best Practice Risk |
| BÜ | Bahnübergang |
| BÜSA | Bahnübergangssicherungsanlage |

C

| | |
|-----------------|---|
| C _{jk} | Reduktionsfaktoren (in der Risikoformel) |
| ca. | circa |
| CENELEC | Comité Européen de Normalisation Electrotechnique (Europäisches Komitee für elektrotechnische Normung) |
| CSM | Common Safety Methods (gemeinsame Sicherheitsmethoden) |
| CST | Common Safety Targets (gemeinsame Sicherheitsziele) |
| CT | Corporate Technologie (Siemens AG) |

D

| | |
|----------------|--|
| D | D-Zug (Zuggattung) |
| D _j | Gefährdungsdauer (in der Risikoformel) |
| DB AG | Deutsche Bahn Aktiengesellschaft |
| d. h. | das heißt |
| DIN | Deutsches Institut für Normung |
| DKE | Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE |
| Dr. | Doktor (Titel) |

E

| | |
|----------|--|
| E | Energie |
| E_i | Bezugsgröße (in der Risikoformel) |
| E_{ij} | Aussetzungsdauer (in der Risikoformel) |
| EBA | Eisenbahn-Bundesamt |
| EBO | Eisenbahn-Bau- und Betriebsordnung |
| EC | Euro City (Zuggattung) |
| EC | European Commission (Europäische Kommission) |
| ECSAG | ERTMS Core SRS Assessment Group |
| Ef | Einschätzungsfehler |
| EG | Europäische Gemeinschaft |
| EMV | Elektromagnetische Verträglichkeit |
| EN | Europäische Norm |
| engl. | Englisch |
| ERA | European Railway Agency (Europäische Eisenbahnagentur) |
| ERTMS | European Rail Traffic Management System (zukünftiges System für Management und Steuerung des Eisenbahnverkehrs auf den Strecken der Transeuropäischen Netze) |
| ESiV | Eisenbahn-Sicherheitsverordnung |
| ESTW | Elektronisches Stellwerk |
| ETA | Event Tree Analysis (Ereignisbaumanalyse) |
| ETCS | European Train Control System (Europäisches Zugsicherungssystem) |
| EU | Europäische Union |
| EUV | Eisenbahn-Untersuchungsverordnung |

F

| | |
|----------|--|
| f | Versagenhäufigkeit (in BP-Risk) |
| ff | folgende (Zitat) |
| F_{ik} | Fatality (Wahrscheinlichkeit eines Todesfalls - in der Risikoformel) |
| FBS | Functional Breakdown Structure (Funktionsstruktur) |
| Fdl | Fahrdienstleiter |
| Fe | Fahrerlaubnis (Zuglaufmeldung beim Zugleitbetrieb) |
| FFB | Funk-Fahr-Betrieb |
| FHA | Functional Hazard Analysis (Verfahren aus der Luftfahrt) |
| FMEA | Failure Modes and Effects Analysis (Ausfalleffektanalyse) |
| FMECA | Failure Modes, Effects and Criticality Analysis |
| FRS | Functional Requirement Specification (Funktionale Anforderungsspezifikation) |
| FsE | Fahrwegsicherungsmeldung (Zuglaufmeldung beim Zugleitbetrieb) |
| FTA | Fault Tree Analysis (Fehlerbaumanalyse) |
| Fü | Fernüberwacht |
| FV-NE | Fahrdienstvorschrift der Nichtbundeseigenen Eisenbahnen |

G

| | |
|-------|--|
| g (G) | Gefahrenabwehr (in BP-Risk) |
| G | Güterverkehrsstrecke |
| G50 | Streckenstandard – Güterverkehrsstrecke (Leit-v. < 50km/h) |
| GAME | Globalement Au Moins Equivalent (französisches Risikoakzeptanzkriterium) |
| ggf. | gegebenenfalls |

H

| | |
|-----|-------------------------------|
| h | Stunde (Zeit) |
| H | Hazard (Gefährdung) |
| HGV | Hochgeschwindigkeitsverkehr |
| Hp | Hauptsignal |
| HR | Hazard Rate (Gefährdungsrate) |

I

| | |
|--------------|---|
| IC | Inter City (Zuggattung) |
| ICE | Inter City Express (Zuggattung) |
| i. d. R. | in der Regel |
| IEC | International Electrotechnical Commission (Normungsgremium für Elektrotechnik) |
| IET | Institution of Engineering and Technology |
| IfEV | Institut für Eisenbahn und Verkehrssicherung |
| I MO RA RD I | Industry Mobility Rail Automation Research and Development Integrity (Siemens AG) |
| IR | Inter Regio (Zuggattung) |
| IRF | Individual Risk of Fatality (Individuelles Todesrisiko – in der Risikoformel) |
| IRSE | Institution of Railway Signal Engineers |
| ISO | Internationale Organisation für Normung (Vereinigung der Standardisierungsgremien) |
| ITC | Internationales Technisches Komitee (der IRSE) |

K

| | |
|-------|------------------------------|
| K | Kritikalität (in BP-Risk) |
| Kfz | Kraftfahrzeug |
| KoRil | Konzern-Richtlinie der DB AG |
| KR | Kollektives Risiko |
| km/h | Kilometer pro Stunde |

L

| | |
|-----|--------------------------|
| LZB | Lineare Zugbeeinflussung |
|-----|--------------------------|

M

| | |
|----------|--|
| m (M) | menschliche Gefahrenabwehr (in BP-Risk) |
| m | Masse |
| M | Mischverkehrsstrecke |
| MAIS | Maximum Abbreviated Injury Scale (Schweregrad Tabelle) |
| mf | mittlerer Fehler |
| min | Minute (Zeit) |
| MSc | Master of Science |
| MGs | Mindestens Gleiche Sicherheit (deutsches Risikoakzeptanzkriterium) |
| MODTrain | Modular Train (EU-Förderprojekt) |
| MMI | Man-Machine-Interface (Mensch-Maschine-Schnittstelle) |
| MMUS | Mensch-Maschine-Umwelt-System |

N

| | |
|----------------|--------------------------------------|
| N _i | Benutzerprofil (in der Risikoformel) |
| NE | Nichtbundeseigene Eisenbahnen |
| NBS | Neubaustrecke |
| NIV | New International Version (Bibel) |
| NRC | Nuclear Regulatory Commission |

P

| | |
|------|---|
| P | Personenverkehrsstrecke |
| P160 | Streckenstandard – Personenverkehrsstrecke (Leit-v: 121 – 160 km/h) |
| P230 | Streckenstandard – Personenverkehrsstrecke (Leit-v: 161 – 230 km/h) |
| P300 | Streckenstandard - Hochgeschwindigkeitsstrecke (Leit-v: > 230km/h) |
| PRA | Probabilistic Risk Analysis |
| prEN | Europäische Vornorm |
| Prof | Professor (Titel) |
| PSA | Probabilistische Sicherheitsanalyse (in der Kernkraft) |
| PZB | Punktförmige Zugbeeinflussung |

R

| | |
|--------|--|
| R | Risiko |
| R | Regionalverkehrsstrecke |
| R80 | Streckenstandard – Regionalverkehrsstrecke (Leit-v: 51 – 100 km/h) |
| R120 | Streckenstandard – Regionalverkehrsstrecke (Leit-v: 81 – 120 km/h) |
| RA | Rail Automation (Siemens AG) |
| RA A | Rail Automation Academy (Siemens AG) |
| RAC-TS | Risk Acceptance Criterion for Technical Systems (europäisches Risikoakzeptanzkriterium für technische Systeme) |
| RAMSS | Reliability, Availability, Maintainability, Security and Safety (Zuverlässigkeit, Verfügbarkeit, Instandhaltung und Sicherheit) |
| RB | Regionalbahn (Zuggattung) |
| RBC | Radio Block Center (Streckenzentrale beim ETCS) |
| RE | Regional Express (Zuggattung) |
| Rf | Rundungsfehler |
| RPN | Risk Priority Number (Risikoprioritätszahl) |
| RRF | Risikoreduktionsfaktor |

S

| | |
|-----------------|--|
| s (S) | Schadensausmaß (in BP-Risk) |
| S' | Vergleichsparameter Schadensausmaß |
| S. | Seite (Literaturverzeichnis) |
| S _{ik} | Schadensausmaß (kollektives Risiko) |
| SAE | Society of Automotive Engineers (amerikanisches Standardisierungsinstitut der Verkehrstechnologie) |
| SE | Stadtexpress (Zuggattung) |
| SGV | Schienengüterverkehr |
| Sifa | Sicherheitsfahrschaltung (Totmannknopf) |
| SIL | Safety Integrity Level (Sicherheitsanforderungsstufe) |
| SPFV | Schienenpersonenfernverkehr |
| SPNV | Schienenpersonennahverkehr |
| SRS | System Requirement Specification (Anforderungen an Systemspezifikation) |
| STM | Specific Transmission Module |
| SZB | Signalisierter Zugleitbetrieb |

T

| | |
|------------|---|
| t (T) | Masse in Abhängigkeit der Zuggattung (in BP-Risk) |
| t | Tonnen (Gewichtseinheit) |
| Tf | Triebfahrzeugführer |
| Tfz | Triebfahrzeug |
| THR | Tolerable Hazard Rate (tolerierbare Gefährdungsrate) |
| TR | Technical Report (Technischer Bericht) |
| TSI | Technische Spezifikation für Interoperabilität |
| TSI CCS HS | Technical specification of interoperability - command control and signaling - high speed (TSI für Zugsteuerung, Zugsicherung und Signalgebung im HGV) |
| TSI RST | Technical specification of interoperability – rolling stock (TSI für Fahrzeuge) |
| TU | Technische Universität |

U

| | |
|------------------|---|
| u | Umrechnungsfaktor |
| u. a. | unter anderem |
| ÜS | Überwachungssignal |
| ÜS _{oE} | Überwachungssignal mit optimierter Einschaltung |
| UNIFE | Union des Industries Ferroviaires Européennes (Europäischer Verband der Bahnindustrie) |
| US | United States (of America) |

V

| | |
|----------------|--|
| v (V) | Geschwindigkeit (maßgebliche Geschwindigkeit in BP-Risk) |
| V _R | Reisegeschwindigkeit |
| vE | vorsichtige Einfahrt (Verfahren im ZLB) |
| VDA | Verband der Automobilindustrie |
| VDE | Verband der Elektrotechnik Elektronik Informationstechnik e.V. |
| VDV | Verband Deutscher Verkehrsunternehmen |
| Ve | Verlassensmeldung (Zuglaufmeldung beim Zugleitbetrieb) |

W

| | |
|----------------|---|
| W | Werteberreich |
| w _k | Konfrontationswahrscheinlichkeit (bei Hinzen) |
| Wk | Wahrscheinlichkeit |

Z

| | |
|-------|-----------------|
| Z | Zug |
| z. B. | zum Beispiel |
| Zf | Zugführer |
| Zl | Zugleiter |
| ZLB | Zugleitbetrieb |
| Zp/d | Zugpaar pro Tag |
| z. T. | zum Teil |
| z. Z. | zurzeit |

Anhang C: TSI

Ein Ziel der europäischen Gemeinschaft ist unter anderem der Auf- und Ausbau der transeuropäischen Netze der Verkehrsinfrastruktur. Für den Eisenbahnsektor hat der Europäische Rat am 23. Juli 1996 mit der Annahme der Richtlinie 96/48/EG (/47/) über die Interoperabilität des transeuropäischen Hochgeschwindigkeitsbahnsystems (HGV) eine erste Maßnahme getroffen. Mit der am 19. März 2001 erlassenen Richtlinie 2001/16/EG (/48/) über die Interoperabilität des konventionellen Eisenbahnsystems werden mit der Richtlinie 96/48/EG gemeinschaftliche Verfahren für die Erarbeitung und Annahme von Technischen Spezifikationen für die Interoperabilität (TSI) sowie gemeinsame Vorschriften für die Bewertung der Konformität mit diesen Spezifikationen eingeführt. Die beiden Interoperabilitätsrichtlinien 96/48/EG und 2001/16/EG wurden durch die Richtlinien 2004/50/EC (/53/) vom 29. April 2004 und die Richtlinie 2007/32/EG (/54/) vom 1. Juni 2007 geändert.

Diese EG-Richtlinien, die von den einzelnen Mitgliedsstaaten in nationales Recht umgesetzt werden müssen, haben das transeuropäische Eisenbahnsystem in funktionale Teilsysteme unterteilt, um für diese grundlegende Anforderungen festzulegen. Dabei wird das bestehende Eisenbahnsystem definiert als *„System, das durch die Strecken und ortsfeste Anlagen umfassenden Eisenbahninfrastrukturen des vorhandenen Eisenbahnnetzes und durch die auf diesen Infrastrukturen verkehrenden Fahrzeuge sowie durch die bestehenden Betriebsvorschriften gebildet wird“* (/51/, Def. 3.5). Bislang sind die in folgender Tabelle zusammengefassten TSIs ausgearbeitet worden, welche laut CSM-Recommendation (/59/, Artikel 8) europaweit als anerkannte Regeln der Technik gelten. Alle genannten Richtlinien sowie die TSIs sind im Internet unter <http://www.eisenbahn-cert.de> veröffentlicht.

| Teilsystem | Abkürzung (engl.) | Richtlinie (TSI) | |
|--|----------------------|----------------------------|--|
| | | Konventioneller Verkehr | HGV Verkehr |
| Infrastruktur | INS | | 2002/732/EG |
| Energie | ENE | | 2002/733/EG |
| Zugsteuerung, Zugsicherung und Signalgebung | CCS | 2006/679/EG | 2002/731/EG ersetzt durch 2006/860/EG |
| Fahrzeuge | RST | | 2002/735/EG |
| Instandhaltung | MAI | | 2002/730/EG |
| Betrieb | OPE | 2006/920/EG | 2002/734/EG |
| Telematikanwendungen | TAF | Verordnung (EG) | |
| Fahrzeuge - Güterwagen | WAG | 2006/861/EG | |
| Fahrzeuge - Lärm | NOI | 2006/66/EG | |

Anhang D: Streckenstandards

Tabelle: Zusammenstellung Streckenstandards (vereinfacht nach /37/)

| Strecken- standard | Leitgeschwindigkeits- stufen | Optimierungs- kriterien | Streckenauslastung (Betriebsprogramm) | |
|-----------------------|---------------------------------|----------------------------------|--|-------------|
| [-] | [km/h] | [-] | Obergrenze (Zielgröße) | Untergrenze |
| | | | [Zp/d] | |
| P 300 (NBS) | 231 – 300 | HGV | 120 | 40 |
| P 230 (ABS) | | Schneller SPFV | 120 | 40 |
| M 230 (ABS) | 161 - 230 | Mischverkehr | 150 | 60 |
| P 160 I | 121 – 160 | Schneller SPFV und SPNV | 120 | 70 |
| P 160 II | | | 60 | 40 |
| M 160 | | Mischverkehr | 150 | 40 |
| G 120 | 81 – 120 | Güterverkehr | 100 | 40 |
| R 120 | 81 – 120 | SPNV | 50 | 25 |
| R 80 | 51 – 100 | SPNV | 25 | 18 |
| G 50 | 50 | regionaler SPNV | 10 | |
| | 50 – 80 | Verbindungskurven, -strecken* | - | |

* Verbindungskurven, -strecken von 0,5 km bis ca. 3 km Länge, die in keinen übergeordneten Standard einteilbar sind.

Tabelle: Streckenkategorien mit Infrastrukturmerkmalen (vereinfacht nach /40/)

| Strecken- kategorie | Infrastrukturmerkmale | | | | |
|-------------------------------------|----------------------------|------------------|------------------|--|--|
| | Vmax- Bereich [km/h] | Anzahl Gleise | Ober- leitung | LST | Oberbau/ Grundsätze |
| FP und F1 Fernstrecke | 201 - 300 | 2 | Ja | CIR-ELKE ⁷⁴ , Zugfunk | Keine BÜs, Reisendensicherungs- systeme an Bahn- steigen, besondere Wei- chen für $v_{\max} > 200$ km/h |
| F2 Fernstrecke | 161 - 200 | 2 | Ja | Hauptsignal- Vorsignal, LZB, Zugfunk | Keine BÜs, Reisenden- warnsysteme an Bahnstei- gen, besondere Weichen für $v_{\max} > 160$ km/h |
| F3 – F6 Fernstrecke | 101 - 160 | 1 oder 2 | Ja | Hauptsignal- Vorsignal, Zugfunk | BÜs |
| Z1 Zulaufstrecke | 51 – 100 | 1 | Ja | Hauptsignal- Vorsignal, Signali- sierter ZLB | BÜs |
| Z2 Zulaufstrecke | bis 50 | 1 | Ja | keine | Einfachste Anforderungen |
| S1 – S3 Stadtschnell- verkehr | bis 120 | 2 | Gleich- strom | Hauptsignal- Vorsignal, Zugfunk | S-Bahn Anforderungen |

⁷⁴ Computer Integrated Railroading – Erhöhung der Leistungsfähigkeit im Kernnetz der Eisenbahn (CIR-ELKE) = eine Weiterentwicklung der Linienförmigen Zugbeeinflussung (LZB).

Anhang E: Funktionsliste

| CODE | | | | Function (prEN) | Example/ Explanation (prEN) | Funktion (DE) | Beispiele/ Erläuterungen (DE) | Interface (Schnittstelle) | Comments (Kommentare) |
|------|---|--|--|---|---|--|---|------------------------------|--|
| B | B | | | Arrange interior space | Interior design | Räume aufteilen, gestalten, verkleiden | Trenn- oder Schirmwände, Innentüren, Verkleidungen | no interface | |
| B | C | | | Carry and enclose the load | (including people and equipment) | Transportgut tragen/ aufnehmen/ umschließen | Fahrzeugkasten, Einhausung, um Reaktionskräfte aufzunehmen | carbody | |
| B | D | | | Protect in case of crash | | Aufprall schützen | Aufkletterschutz, Energieabsorptionselemente im Falle eines Crashes, strukturelle Wagenkastenfestigkeit | carbody | |
| B | E | | | Protect against fire | fire alarm system, fire extinguishing system | Vor Feuer schützen | Brandschutzkonzept | no interface | Brandmelde- und -löschanlage |
| C | B | | | Provide safe and comfortable sitting, lying and standing positions | seats, couchettes, measures taken to ensure safe standing room | Sichere & komfortable Aufenthalts- & Sitzlandschaften bereitstellen | Sitze, Liegen, Vorkehrungen für sicheres Stehen | no interface | |
| C | C | | | Provide external view | windows, cameras | Blick-/Beobachtungsmöglichkeit nach Außen sicherstellen | Fenster, ggf. auch Kameras | windows | |
| C | D | | | Provide interior lighting | interior lighting | Innenbeleuchtung bereitstellen | Innenbeleuchtung | no interface | |
| C | E | | | Provide proper climate | heater, air conditioning, climate control | Fahrzeugklimatisierung bereitstellen | Heizung, Lüftung, Klimatisierung | no interface | |
| C | F | | | Provide public address, passenger information, intercommunication and entertainment | labelling, timetable information, audio and video entertainment | Bereitstellen von "public address", Passagierinformation, Intercom & Entertainment | Kommunikation, Beschriftung, Fahrplaninfo, Audio- und Videounterhaltung | no interface | auch sicherheitsrelevante Warnhinweise der Crew an die Passagiere durch Lautsprecherdurchsagen |

| CODE | | | | Function (prEN) | Example/ Explanation (prEN) | Funktion (DE) | Beispiele/ Erläuterungen (DE) | Interface (Schnittstelle) | Comments (Kommentare) |
|------|---|---|--|---|--|--|--|--|--|
| C | G | | | Provide surveillance (for passenger and load) | interior video control (CCTV) | Passagier- / Ladungsüberwachung ermöglichen | CCTV (Closed Circuit Tele Vision) system | no interface | interne Videoüberwachung der Passagier- und Laderäume |
| C | H | | | Provide sanitary services | restroom, lavatory, | Sanitärfunktionen bereitstellen | Toiletten, Waschräume | no interface | |
| C | J | | | Provide catering | restaurant, bistro, galley | Gastronomische Funktionen bereitstellen | Restaurant, Bistro, Galley | no interface | |
| C | K | | | Provide additional service related functions | ticket machine, passenger counter | Sonstige Servicefunktionen bereitstellen | Fahrkartenautomaten | no interface | Fahrgastzähleinrichtung |
| C | L | | | Provide tilting ability | tilting ability to improve comfort | Neigung aus Komfortgründen zur Limitierung der Querbeschleunigung im Wagenkasten | Bogenschnelles Fahren (Neigetechnik) | carbody | |
| C | L | B | | Control tilting | detect train position/speed | Neigungsvorgang überwachen | Steuerung Neigetechnik; Positions- und Geschwindigkeitsüberwachung | vehicle control system | |
| C | L | C | | tilt the vehicle | propulsion for tilting | Fahrzeugkasten neigen | Neigeantrieb | carbody | aktive Neigetechnik mit Antrieb |
| C | L | E | | ensure track clearance | supervision and protection | ausreichendes Lichtraumprofil für Neigung sicherstellen | Streckenprofilüberwachung | gauge envelope | Lichtraumprofil im Zusammenhang mit der Neigetechnik; durch die Neigung des Wagenkastens kann das Lichtraumprofil verletzt werden. |
| D | B | | | Provide external access | functions associated with the management of the external doors | Zugang von außen ermöglichen | Türen, Notausstiege, Tritte, Treppen, Haltegriffe, Geländer, Laderampen, Rollstuhlhilfe, Laufstege, rutschfeste Beläge | sensoric, door control, passengers, MMI, ATC | Funktionen, verbunden mit dem Management der Außentüren |

| CODE | | | | Function (prEN) | Example/ Explanation (prEN) | Funktion (DE) | Beispiele/ Erläuterungen (DE) | Interface (Schnittstelle) | Comments (Kommentare) |
|------|---|---|--|---|---|--|--|------------------------------------|---|
| D | B | B | | Release external doors | Enable the doors to be opened by passengers, driver, ATC (also: velocity of vehicle must be lower than...km/h for door release) | Außentüren lösen | Türöffnung durch Fahrgäste ermöglichen | door control, passengers, MMI, ATC | |
| D | B | E | | Manage door system upon obstacle | Detect obstacle, manage door system according to obstacle detector | Türsystem bei Hindernis managen | Positions- und Zustandserkennung | door control | |
| D | B | F | | Lock external doors | pneumatic control (also in case of failure) | Außentüren verriegeln | | door control | |
| D | B | H | | Enable selective external door opening | in order to make certain vehicles of the train inaccessible | Selektives Öffnen von Außentüren ermöglichen | z.B. um bestimmte Fahrzeuge des Zugs unzugänglich zu halten | door control | |
| D | B | N | | Enable external door opening in emergency | mechanical lever | Öffnen der Außentüren im Notfall ermöglichen | Hebel mit Ausschnitt für Türantrieb und -kontrolle | door control | Erkennung des Öffnungs- und Ableitungssignals zur Zugkontrolle zur Einleitung der Notbremsung / zur Vermeidung des Starts |
| D | C | | | Provide access by internal doors | Doors between vehicles enabling passengers to circulate in the train | Zugang über Innentüren ermöglichen | Türen zwischen den Fahrzeugen, die den Fahrgästen die Bewegung im Zug ermöglichen | no interface | |
| D | D | | | Ensure goods loading & unloading | Hatches, loading compartment doors, filling systems, emptying systems, gravity unloading | Fracht laden und entladen ermöglichen | Luken, Laderaumtüren, Befüllleinrichtungen, Entleereinrichtung, Schwerkraftentladung | doors, openings | Laden und Entladen von Gütern über Türen oder Schüttguteinrichtungen |

| CODE | | | | Function (prEN) | Example/ Explanation (prEN) | Funktion (DE) | Beispiele/ Erläuterungen (DE) | Interface (Schnittstelle) | Comments (Kommentare) |
|------|---|---|--|--|---|--|--|---------------------------|--|
| E | B | | | Enable flexible configuration or towing | Allow free operational configuration of the consists to built up a train | Flexible Konfiguration ermöglichen | Freies Zusammenstellen von Zugteilen im Betrieb | coupler | |
| E | B | B | | Coupling | Manage and prepare coupling, open cover, configure coupling mode, execute and complete coupling | Kuppeln steuern | | coupler | Actuating coupling process |
| E | B | C | | Uncoupling | manage and prepare uncoupling | Entkuppeln steuern | | coupler | Actuating uncoupling process |
| E | B | D | | Transmit forces | via coupler, protect force transmission elements | Kräfte über Kupplung übertragen | Zug- und Stoßkräfte | coupler | |
| E | B | E | | Connect signals | utilities, power service lines | Signalleitungen, Energie- und Hilfsenergieleitungen verbinden | Zugsteuerleitungen, Bussysteme, Druckleitungen | coupler | Electric and pneumatic coupling & uncoupling |
| E | B | F | | Detect uncoupling | ensure adequate reaction on unintended uncoupling | Zugtrennung erkennen und darauf reagieren | Rückmeldung zum Kuppelstatus (gekuppelt, entkuppelt) | coupler | |
| E | C | | | Allow intercar passenger & goods circulation | Gangways | Passagier- und Nutzlasttransfer zwischen den Wagen ermöglichen | Fahrzeugübergang, Mittelpufferkupplung | coupler | |
| F | B | | | Provide electrical energy for traction | power supply line | Traktionsenergie bereitstellen | Stromzuführung inkl. Rückstromführung | pantograph | Oberleitung, aber auch mittels Generator von Diesel |
| F | C | | | Provide electrical energy for auxiliaries | | Elektrische Energie für Hilfsbetriebe bereitstellen | Bordnetzumrichter, Bordnetzgenerator Hilfsdiesel, Hauptluftpresser, Hilfsluftpresser | pantograph | Bordnetzumrichter wird aus dem Zwischenkreis oder der Oberleitung gespeist |
| F | D | | | Provide fluid energy for traction | This function covers hydraulic and pneumatic systems. | Strömungsenergie für Traktion bereitstellen | Transformer, Stromrichter, Dieselmotor, Hydraulik | | |

| CODE | | | | Function (prEN) | Example/ Explanation (prEN) | Funktion (DE) | Beispiele/ Erläuterungen (DE) | Interface (Schnittstelle) | Comments (Kommentare) |
|------|---|---|---|---|---|---|--|----------------------------------|-----------------------|
| F | E | | | Provide fluid energy for auxiliaries | This function covers hydraulic and pneumatic systems | Strömungsenergie für Hilfsbetriebe bereitstellen | | | |
| F | F | | | Provide mechanical energy for traction | | Mechanische Energie für Traktion bereitstellen | | | |
| F | G | | | Provide mechanical energy for auxiliaries | | Mechanische Energie für Hilfsbetriebe bereitstellen | | | |
| F | H | | | Provide chemical energy for traction | | Chemische Energie für Traktion bereitstellen | | | |
| G | B | | | Provide acceleration and dynamic brake force | traction motor, transmission | Vortriebskraft und Bremskraft erzeugen | Traktionsstromrichter, Getriebe und Fahrmotor | | |
| G | B | C | | Acquire propulsion demand | propulsion demand from driver, ATO, internal speed control, brake demand for dynamic brake force from brake control | | verarbeitet Traktionsanforderung durch den Tf oder andere Steuerungseinrichtungen (z.B. ATO) innerhalb der Traktionssteuerung weiter | traction control | |
| G | B | C | D | Acquire traction cut-off | | | | vehicle control system | |
| G | C | | | Provide deceleration and keep the train at standstill | braking | Bremsen | Generell die Bremsfunktionalität, inklusive pneumatische Bremse | brake control system, brake pipe | |
| G | C | B | | Get status of braking systems | also: isolate braking devices, | | | brake control system | |

| CODE | Function (prEN) | Example/ Explanation (prEN) | Funktion (DE) | Beispiele/ Erläuterungen (DE) | Interface (Schnittstelle) | Comments (Kommentare) |
|-------|--|--|--|---|---------------------------|--|
| G C C | Acquire brake demand | from: driver, brake control, emergency device, train protection functions, ATP, brake signal transition, internal speed control, passengers and crew | | Bremsanforderungen innerhalb des Fahrzeugs, durch den Tf aber auch z.B. durch die Zugsicherungseinrichtung; auch das Managen des Brake Blendings zwischen den verschiedenen Bremsarten (elektrisches oder mechanisches Bremsen) | brake control system | could be detailed in direct and indirect brake demands by driver |
| G C D | Prioritise brake demand and select braking mode | setup (emergency) brake mode | | | brake control system | |
| G C E | Allocate braking effort | Calculate needed braking effort | | | brake control system | |
| G C F | Handle braking due to train configuration, brake mode and brake demand | i. e. Emergency Brake, Service Brake, Parking Brake | | | brake control system | provide brake command for holding brake or service brake, manage brake blending, request traction cut-off, acquire realized braking effort |
| G C G | Apply and release braking forces | detect non-release of braking forces | | | vehicle control system | |
| G C H | Provide Wheel Slide Protection (WSP) | Detect and control sliding | | | vehicle control system | die WSP-Funktion hebt ggf. den Bremszugriff auf, greift massiv in das Bremssystem ein |
| G D | Improve adhesion | sanding | Kraftschlussbeiwert Rad/Schiene verbessern | Gleitschutz, Sandung, Putzklötze | carriage | |

| CODE | | | | Function (prEN) | Example/ Explanation (prEN) | Funktion (DE) | Beispiele/ Erläuterungen (DE) | Interface (Schnittstelle) | Comments (Kommentare) |
|------|---|---|--|---------------------------------|--|--------------------------------------|--|---------------------------|--|
| H | B | | | Keep the train staff informed | all functionality to inform the train crew about the actual state of the train and its systems | Zugpersonal informieren | alle Funktionen, um das Zugpersonal über den Zustand des Zuges und dessen Systeme zu informieren | MMI | |
| H | C | | | Provide trainwide communication | | Zugweite Kommunikation bereitstellen | betriebliche Kommunikation im Zug oder mit ortsfesten Einrichtungen | KDC | Kommunikation innerhalb des Zuges bzw. zwischen zusammengekuppelten Zügen |
| H | C | B | | Confirm train configuration | Determine train topology and configuration, provide orientation information for coupled elements | Zugtaufe | Zugtaufe zur Bestimmung der Zugkonfiguration (Anzahl, Reihenfolge, Richtung und Eigenschaften der einzelnen Wagen) | ATC, MMI | Daten für das Zugsteuergerät (ZSG); die vorhandenen Wagen und deren Reihenfolge sind notwendig zur Steuerung der Systeme |
| H | C | C | | Transmit data | | Zugbus steuern | Zugang, Datenpriorisierung, QoS | no interface | |
| H | D | | | Manage train modes | Also managing of transitions between train modes | Zugbetriebsart steuern | Steuerung des Fahrzeuges in allen Betriebsphasen | ATP | |
| H | E | | | Allow proper control | This function is related to the interface of the driver to the various subsystems | Einwandfreie Steuerung ermöglichen | allgemeine Bedien- und Steuerungsfunktionen, hauptsächlich durch Tf | MMI | betreffen Funktionen innerhalb des Fahrzeuges |
| H | E | B | | Manage cab control | functions to control the cab and its functionality | Führerstand steuern | Funktionen zur Cabsteuerung und zur Steuerung seiner Funktionalität | ATC, key switch | Schlüsselschalter zum Aufriegeln des Führerstandes (key switch) |

| CODE | | | | Function (prEN) | Example/ Explanation (prEN) | Funktion (DE) | Beispiele/ Erläuterungen (DE) | Interface (Schnittstelle) | Comments (Kommentare) |
|------|---|---|--|--|---|--|---|------------------------------|--|
| H | E | C | | Manage propulsion and brake demand | central functions to control propulsion and brakes | Fahr- / Bremsanforderung steuern | Brems- und Beschleunigungsanforderung; Brake-Blending, bei welchem die Bremssteuerung die elektrische Bremse und die mechanische Bremse steuert | vehicle control system | Übergeordnete Fahr- und Bremssteuerung des Fahrzeugs (durch den Tf, z.B. Fahr-Brems-Hebel) |
| H | E | D | | Manage energy supply | central functions to control battery main switch, main circuit breaker, pantographs | Energieversorgung steuern | Zentrale Funktionen zur Steuerung von Batterie-hauptschalter, Hauptschalter, Pantograph | Interface to F | |
| H | E | E | | Manage appropriate and safe conditions | central functions to control comfort and safety functionality | Geeignete und sichere Bedingungen steuern | Zentrale Funktionen zur Steuerung von Komfort- und Sicherheitsfunktionen | | Bedarfsgerechte Vorhaltung; Schaltwerk, Pulswechselrichter inkl. Steuerungselektronik |
| H | E | F | | Manage access and loading | central functions to control access vial external doors. | Zugang, Be- und Entladen steuern | Türsteuerung | doors | |
| H | E | G | | Manage connecting of vehicles | central functions to control coupling | Kuppeln steuern | Steuerung / Freigabe des Kuppelvorganges | coupler | Zentrale Funktionen zur Steuerung des Zugangs durch die Außentüren |
| H | E | H | | Manage control of train parameters | Enter wheel diameter, manage isolation of devices | Zugparameter einstellen | Zentrale Funktionen zur Steuerung von Zugparametern wie Zeit, Strecke | MMI | |
| H | E | J | | Manage integration of the vehicle in the complete railway system | central functions to control exterior lighting, signalling, traffic lights | Integration in das Eisenbahnsystem steuern | Zentrale Funktionen zur Steuerung der externen Beleuchtung, Signale | carbody | |
| H | F | | | Manage checks before train departure | | Zugselbsttests steuern | | no interface | |

| CODE | | | | Function (prEN) | Example/ Explanation (prEN) | Funktion (DE) | Beispiele/ Erläuterungen (DE) | Interface (Schnittstelle) | Comments (Kommentare) |
|------|---|---|--|-------------------------------------|--|---|--|------------------------------|--|
| H | G | | | Provide diagnostics | | Diagnose bereitstellen | Diagnose von Zug- und Komponentenzuständen | | |
| H | H | | | Assist Troubleshooting | | Fehlersuche unterstützen | | | |
| H | J | | | Supervise driver activity | vigilance button | Fahrer überwachen | Sicherheitsfahr- schaltung (Sifa) | ATP, MMI | |
| H | K | | | Provide juridical data recording | tachograph, trip recorder | Gesicherte Datenauf- zeichnung bereitstellen | Fahrtenschreiber | ATC | Fahrtenschreiber; ähn- lich einer Black-Box in Flugzeugen; evtl. Auf- zeichnung von ATP- und ATO-Daten |
| J | B | | | Guide the train | | Führen des Zuges | Radsatzführung, - anlenkung, auch Spur- wechselradsätze | carriage | |
| J | B | C | | Provide derailment in- formation | | Entgleisungs-information bereitstellen | Detektieren der Entglei- sung eines Zuges mittels Überwachung der rele- vanten onboard Parame- ter mit einer Mindestzu- verlässigkeit in jedem Betriebszustand | carriage, MMI | |
| J | B | D | | Monitor obstacles within track | detect obstacles within clearance gauge | Hindernisse im Gleis überwachen | Überwachen möglicher Hindernisse im Gleis während des Betriebs- einsatzes eines Zuges | KEB | |
| J | B | N | | Prevent derailment | | Entgleisen verhindern | | | |

| CODE | | | | Function (prEN) | Example/ Explanation (prEN) | Funktion (DE) | Beispiele/ Erläuterungen (DE) | Interface (Schnittstelle) | Comments (Kommentare) |
|------|---|---|--|--|---|---|---|------------------------------|--|
| J | C | | | Transmit forces | | Kräfte übertragen | Drehzapfen, Zug-/Druckstange, Wankstütze, Wankstabilisator, Querzentrierung, Fahrwerk- und Fahrzeugkasten-anbindung | carriage | |
| J | D | | | Limit x-y-z acceleration | Assessment of the ride characteristics, assessment of the passenger comfort | Beschleunigung in x-y-z-Richtung limitieren | | CL | |
| J | E | | | Keep vehicle inside gauge envelope | Ensure that the rolling stock used comply with the gauge concerned in all running service condition | Fahrzeug innerhalb der Begrenzungslinie halten | Sicherstellen, dass das Fahrzeug mit der Fahrzeugbegrenzungslinie bei allen Betriebsbedingungen übereinstimmt | carbody | Beurteilung der Laufcharakteristiken, Laufqualität' des Fahrzeuges |
| J | E | B | | Detect and correct tilting movement | | Erkennen und Korrigieren von Neigebewegungen | | CLB | |
| K | B | | | Indicate the presence of the vehicle to others | | Gleisbelegung anderen (Fahrzeugen) anzeigen | Signallichtführung (Schlussignal), Makrofon | carbody | |
| K | B | D | | Indicate the presence by external lights | tail-end signal | Gleisbelegung durch Fzg.-Außenbeleuchtung (Signalisierung) erkennbar machen | z.B. End- und Spitzen-signal | carbody | |
| K | C | | | Provide identification | | Fahrzeugidentifikation ermöglichen | | carbody | |
| K | D | | | Provide operational communication and train/ground data transmission | | Betriebliche Kommunikation und Datenübertragung Zug-/Extern ermöglichen | alle Arten der Kommunikation | LD | |

| CODE | | | | Function (prEN) | Example/ Explanation (prEN) | Funktion (DE) | Beispiele/ Erläuterungen (DE) | Interface (Schnittstelle) | Comments (Kommentare) |
|------|---|---|--|---|--------------------------------|--|---|------------------------------|--|
| K | D | B | | Ensure data interface to trackside signaling system | train antenna | Signaltechnische Beeinflussung des Fahrzeuges gewährleisten; Datenübertragung mit Streckensignalisierung sicherstellen | Steuerstromkreise, Bussysteme | communication system | Interface des Fahrzeugs zu den gleisseitigen Sicherungseinrichtungen (Balisen, Magnete) durch Fahrzeugantennen; die Verarbeitung der Daten erfolgt im ATP/ATC |
| K | D | C | | Provide train to ground communication | train radio, GSM-R | Betriebliche Kommunikation vom Zug nach Extern ermöglichen | Übertragung von Betriebs- und Diagnosedaten | communication system | Zugfunk zwischen Tf und Betriebszentrale oder anderem Personal; Kommunikation zwischen Zug und externen Einrichtungen |
| K | D | D | | Provide ground to train communication | | Datentransfer / Beeinflussbarkeit von Extern zum Zug sicherstellen | Übertragung von Betriebs- und Diagnosedaten | communication system | evtl. löschen, da in KDC enthalten |
| K | E | | | Provide automatic train protection & control | | Automatische Zugsicherung/-steuerung ermöglichen | Fahrerloses Fahren gewährleisten | ATC = ATP + ATO | Die Zugsicherung steuert auch zugintern die Fahr- und Bremsfunktionen, jedoch geschieht dies mittels Input von außen (Balisen oder Gleisschleifen geben einen Signal- oder Geschwindigkeitsbegriff für Streckenabschnitt vor |
| K | E | B | | Provide interface with ATC | | ATC-Schnittstelle bereitstellen | Über ATC in das Gesamtsystem integrieren | ATC | |
| K | F | | | Provide automatic train operation | | Automatischen Zugbetrieb ermöglichen | Eingriff auf Fahr- und Bremssteuerung | | |

| CODE | | | | Function (prEN) | Example/ Explanation (prEN) | Funktion (DE) | Beispiele/ Erläuterungen (DE) | Interface (Schnittstelle) | Comments (Kommentare) |
|------|---|---|--|--|---|--|--|---------------------------|--|
| K | G | | | Ensure proper route selection and route signalling | switch control | Korrekte Fahrwegwahl / Streckensignalansteuerung | Weichensteuerung Vorrangschaltung | switch/signal | KG Funktionsgruppe eher im Nahverkehr |
| K | G | B | | Switch route | device for working the switches | Streckenführung wählen | Weichenstelleinrichtung | switch | |
| K | G | C | | Control signals | activate traffic light signals | Signale steuern und überwachen | Lichtsignalbeeinflussung | signals, level crossing | Streckensignale ansteuern |
| L | B | | | Provide wayside functions | wayside functions | Streckenfunktionen steuern und sichern | Streckenfunktionen | | (Transverse Function Z) |
| L | B | B | | Provide track vacancy detection | track vacancy detection | Gleisschaltmittel, Gleisfreimeldung | Gleisstromkreise, Achszähler | JBD | |
| L | B | C | | Provide positioning information | location balise | streckenseitige Ortung | Balisen (Kilometersteine) | CLB, DBE, KD | |
| L | B | D | | Provide wayside train protection | Eurobalise | streckenseitige Zugbeeinflussung | Balisen, Indusi-Magneten, Kabellinienleiter | KEB | |
| L | B | E | | Provide operational telecommunication | commercial telecommunication system | Betriebsfernmeldeanlagen | Beschallungs- und Wechselsprechanlagen, Melde- und Überwachungssysteme, betriebliche Gefahrenmeldeanlagen, Videotechnik, Zugfunk | KDC, HC | |
| L | B | F | | Control switches | switch control, derailer (track locks) | Bewegliche Fahrweg-elemente sichern | Weichen, Gleissperren, | KGB | |
| L | B | G | | Supervise level crossing | activation, deactivation, monitoring signal | BÜ sichern | Einschaltung, Ausschaltung, Überwachungssignal | KGC | |
| L | B | H | | Show correct proceed aspect | signaling systems | Korrektes Fahrsignal anzeigen | Stellbare Signale | KGC | auch Gleisabschluss (Prellbock, Hemmschuh) |

Anhang F: Berechnung BÜ

| Standard | # BÜ* 20317,00 | Netz | Anteil (%) | Anteil (%) | Betriebskm* 34128,4 | # BÜ/km |
|-----------------|-------------------|-----------|------------|-------------|------------------------|---------|
| P 300 | | H | 2,13 | | 728,35 | |
| HGV | | | | | 728,35 | |
| P 230 | | H | 2,13 | | 728,35 | |
| M 230 | | M | 4,88 | | 1.664,80 | |
| SPFV230 | | | | | 2.393,15 | |
| | | | | % | HGV + SPFV | |
| | | | | 9,15 | 3.121,50 | |
| | | | | | km neu | |
| | | | | | 31.006,90 | |
| P 160 I | | H | 2,13 | 2,35 | 728,35 | |
| P 160 II | | H | 2,13 | 2,35 | 728,35 | |
| M 160 | | M | 4,88 | 5,37 | 1.664,80 | |
| SPFV160 | 899,91 | | | | 3.121,50 | 0,33 |
| G 120 | | M | 4,88 | 5,37 | 1.664,80 | |
| R 120 | | M + R | 30,49 | 33,56 | 10.405,00 | |
| SPNV120 | 3882,68 | | | | 12.069,80 | 0,33 |
| R 80 | | M + S + R | 35,37 | 38,93 | 12.069,80 | |
| SPNV80 | 11929,21 | | | | 12.069,80 | 1,00 |
| G 50 | | G | 10,98 | 12,08 | 3.745,80 | |
| SGV | 3605,21 | | 100,00 | 100,00 | 3.745,80 | 1,00 |

| Beschreibung | "Netz 21" | % | km |
|--|-----------|--------|-------|
| Leistungsnetz für weiträumigen Personenfernverkehr | H-Netz | 8,54 | 3500 |
| Leistungsnetz für den Güterverkehr | G-Netz | 10,98 | 4500 |
| Artreine Netze für die S-Bahn | S-Netz | 4,88 | 2000 |
| Ergänzende Netze im Mischverkehr | M-Netz | 24,39 | 10000 |
| Regionalnetze, teilweise mit "Shortline"-Charakter | R-Netz | 51,22 | 21000 |
| | | 100,00 | 41000 |

*Angaben nach /36/

Anhang G: VDV-Schrift 752

Aufgrund von Zusammenstößen auf eingleisigen Strecken mit Zugleitbetrieb entwickelte der Verband Deutscher Verkehrsunternehmen e.V. (VDV) unter Einbeziehung verschiedener Eisenbahnverkehrs- und –Infrastrukturunternehmen die VDV-Schrift 752 (/116/), mit deren Hilfe geeignete Betriebsverfahren und die Notwendigkeit einer technischen Unterstützung ermittelt werden können (/2/). Den Hauptteil der VDV-Schrift 752 bildet eine Bewertungsmethode, bei der auf Basis unterschiedlich gewichteter Einflussfaktoren eine Gesamtzahl ermittelt wird, die als Maß für die Eignung der verschiedenen Betriebsverfahren dient. Neben verschiedenen Problemen in der Anwendung (siehe dazu /108/, Seite 25 - 27) ist auch unklar, nach welchen Kriterien oder Modellen die Faktoren und vor allem deren Gewichtung innerhalb dieser Bewertungsmethode gewählt wurden. Beispielsweise wurden die Bewertungsfaktoren, die Streckeneinteilung, die Grenzen der Punktebereiche auf Basis empirischer Erhebungen und Expertenwissen aufgestellt, was sie wenig nachvollziehbar macht. Die Ergebnisse der dazu durchgeführten Umfragen sind nicht öffentlich, so dass auch die Begründung und die Randbedingungen nicht bekannt sind⁷⁵.

Eine geänderte Fassung der VDV-Schrift wurde im März 2004 eingeführt, wobei das EBA den Geltungsbereich auf die Eisenbahnen des Bundes erweiterte. Bei den NE-Bahnen stellt die VDV-Schrift 752 eine Entscheidungshilfe dar. Im Gegensatz dazu ist das Bewertungsverfahren für die Eisenbahnen des Bundes nach Anweisung des EBA bindend und wurde dabei mit ergänzenden und verschärften Bestimmungen versehen, da der ZLB mit alleiniger menschlicher Sicherheitsverantwortung als nicht mehr zeitgemäß angesehen wird (nach /108/, Seite 23, 24). Eine wesentliche Änderung der neusten Fassung vom März 2004 gegenüber der vorherigen, ist die Forderung einer technischen Unterstützung für den ZLB. Dazu heißt es: *„Sofern auf Strecken mit Reisezugbetrieb [...] Zugleitbetrieb erstmalig als Betriebsverfahren vorgesehen ist, sollen⁷⁶ einfache technische Systeme die sichere Durchführung des Betriebes unterstützen. Als Mindestanforderung für derartige technische Systeme gilt eine punktförmige Zugbeeinflussung. Dabei sind die Bahnhofsköpfe mit Einwirkungsstellen zur Auslösung einer Zwangsbremse auszurüsten, die durch einen streckenabschnittsbezogenen Schlüssel freigegeben werden, der wie im Stabblockverfahren zu handhaben ist“* (/116/).

Die VDV-Schrift 752 muss als anerkannte Regel der Technik für die Auswahl geeigneter Betriebsverfahren streckenbezogen berücksichtigt werden, für den jeweiligen Anwendungsfall sollten aufgrund der oben genannten Probleme jedoch auch gesonderte Bewertungsverfahren herangezogen werden.

⁷⁵ „Die VDV-Schrift 752 ist auch unter Fachleuten nicht unumstritten, da zwar die Gesamtzahl der Züge berücksichtigt wird, jedoch nicht die Zahl der Züge, die sich gleichzeitig auf der Zugleitstrecke befinden. Letzteres ist für die Wahrscheinlichkeit von Zusammenstößen viel entscheidender als die Gesamtzahl der Züge pro Tag.“

⁷⁶ In der Praxis werden derartige Soll-Bestimmungen heute als ‚Muss‘ angesehen, wenn nicht schwerwiegende Gründe dagegen sprechen.

Anhang H: Funktionen ZLB

| | | Funktion (DE) | Beispiel/Erläuterung | Kommentar |
|----------|----------|---|---|--|
| K | B | Gleisbelegung anderen (Fahrzeugen) anzeigen | Signallichtführung Schlussignal, Makrofon | in Funktion LBB und LBH enthalten (z.B. für Signal „Kommen“). |
| K | C | Fahrzeugidentifikation ermöglichen | | Die Identifizierung des Fahrzeugs gehört im ZLB zu den Zuglaufmeldungen, in denen der Zf die Zugnummer an den ZI übermittelt. |
| K | D | Betriebliche Kommunikation und Datenübertragung Zug-/Extern ermöglichen | alle Arten der Kommunikation | Im ZLB besteht die betriebliche Kommunikation aus den Zuglaufmeldungen zwischen ZI und Zf (bzw. Zugmeldungen zwischen ZI und Nachbar-Fdl), diese wird i.d.R. über Zugfunk ermöglicht (siehe auch Funktion LBF); Weginformationen werden durch nicht stellbare Signale (H-Tafel, Trapeztafel, usw.) bzw. durch den Buchfahrplan (Informationen über Halt, Kreuzungen usw.) und auch durch die Fe übermittelt; Geschwindigkeitsinformationen werden nur durch den Buchfahrplan bereitgestellt. |
| K | E | Zugsicherung/-steuerung ermöglichen | Fahrerloses Fahren gewährleisten | Die Zugsicherung (Fahrgrenzen und Geschwindigkeit überwachen) übernimmt im ZLB der Tf. |
| K | F | Zugbetrieb ermöglichen | Eingriff auf Fahr- und Bremssteuerung | |
| K | G | Korrekte Fahrwegwahl/ Streckensignalansteuerung gewährleisten | Weichensteuerung Vorrangschaltung | Die korrekte Fahrwegwahl im ZLB besteht aus dem korrekten Einstellen des Fahrwegs auf unbesetzten Bahnhöfen durch den Zf. |
| L | B | B Gleisschaltmittel, Gleisfreimeldung bereitstellen | Gleisstromkreise, Achs-zähler | Die Gleisfreimeldung und die Ortung erfolgt im ZLB durch die Zuglaufmeldungen des Zugführers (Ankunft-, Verlassens-, Fahrwegsicherungs- und Abstellmeldung). |
| L | B | C streckenseitige Ortung bereitstellen | Balisen (Kilometersteine) | |
| L | B | D streckenseitige Zugbeeinflussung bereitstellen | Balisen, Indusi-Magneten, ... | Die Zugsicherung (Fahrgrenzen und Geschwindigkeit überwachen) übernimmt im ZLB der Tf (siehe Funktion KE und KF). |
| L | B | E Betriebsfernmeldeanlagen bereitstellen | Wechselsprechanlagen, Meldesysteme, Zugfunk | I.d.R. werden die Zuglaufmeldungen über Zugfunk (oder Streckenfernsprecher) gegeben, das öffentliche Mobilfunknetz kann auch genutzt werden. |
| L | B | F Bewegliche Fahrweg-elemente sichern | Weichen, Gleissperren | Das Sichern des Fahrwegs wird im ZLB bei unbesetzten Bahnhöfen durch den Zf gewährleistet (durch das Verschließen der Weichen oder der Hebelbank). |
| L | B | G BÜ sichern | Einschaltung, Ausschaltung, Überwachungssignal | nicht relevant, da im Rahmen von ZLB keine Sicherheitsbetrachtung von BÜs berücksichtigt wird (eigene Risikoanalyse). |
| L | B | H Korrektes Fahrsignal anzeigen | Stellbare Signale | Die Zulassung der Fahrt wird mittels Fe durch den ZI (bzw. Fdl in Funktion des ZI) gegeben. Bei Zugkreuzungen kann die Zustimmung zur Fahrt auch durch das Signal „Kommen“ gegeben werden. |

Literaturverzeichnis

- /1/ ACKERMANN, T.
Die Bewertung der Pünktlichkeit als Qualitätsparameter im Schienenpersonenverkehr auf Basis der direkten Nutzenmessung, Forschungsarbeit des Verkehrswissenschaftlichen Instituts an der Universität Stuttgart, Bericht 21, 1998.
- /2/ BAUM, K-D.
Die VDV-Schrift 752 als Entscheidungshilfe für den Eisenbahnbetriebsleiter, Vortrag bei der 11. Fachtagung „Leiten und Sichern auf Nebenstrecken – Probleme und Visionen“ am 26.04.2005 an der TU Dresden, Professur für Verkehrssicherungstechnik.
- /3/ BECKER, H.
Ist die Eisenbahn im Güterverkehr noch konkurrenzfähig?
<http://members.tripod.com/~HubertB/konkureb.pdf>, Stand: März, 2008.
- /4/ BEDFORD, T.; COOKE, R.
Probabilistic risk analysis: foundations and methods, Cambridge University Press, 2001, <http://assets.cambridge.org/9780521773201/sample/9780521773201ws.pdf>.
- /5/ BORMET, J.
Anforderungen des Betreibers an den Life-cycle in der Fahrwegsicherungstechnik, Signal + Draht, Heft 1+2/2007, S. 6 – 16.
- /6/ BPV CONSULT GMBH
Nahverkehrsplan für den Schienenpersonennahverkehr im Freistaat Thüringen, BPV Consult GmbH (Erfurt / Koblenz), 2003.
- /7/ BRABAND, J. (2003)
Improving the Risk Priority Number Concept, Journal of System Safety, Nr. 3/2003, S. 21 – 23.
- /8/ BRABAND, J. (2004)
Sicherheitsanalyse technischer Systeme, Vorlesungsunterlagen Sommersemester 2004, Institut für Eisenbahnwesen und Verkehrssicherung, TU-Braunschweig 2004.
- /9/ BRABAND, J. (2005A)
Risikoanalysen in der Eisenbahn-Automatisierung, Eurailpress Edition Signal + Draht, Hestra-Verlag, Hamburg, 2005.
- /10/ BRABAND, J. (2005B)
Ein semi-quantitativer Ansatz zur Risikoanalyse in der Eisenbahnautomatisierungstechnik, Eurailpress, Signal + Draht, Heft 10/2005, S. 6 – 14.
- /11/ BRABAND, J. (2006A)
Risikoanalyse technischer Systeme, Vorlesungsunterlagen Wintersemester 2006/07, Institut für Eisenbahnwesen und Verkehrssicherung, TU-Braunschweig 2006.
- /12/ BRABAND, J. (2006B)
Risk Assessment: As Simple as Possible (and No Simpler), Proceedings IET System Safety Conference 2006 in London, S. 285 – 300.

- /13/ BRABAND, J. (2006C)
Funktionale Sicherheit, Handbuch Eisenbahninfrastruktur, Hrsg. Lothar Fendrich, Springer Verlag, 2006, Kapitel 14, S. 649 - 699.
- /14/ BRABAND, J. (2007A)
A proposal for common safety methods for technical systems in European railways, Eurailpress, Signal und Draht, Heft 4/2007, S. 34 – 37.
- /15/ BRABAND, J. (2007B)
Risikoprioritätszahlen als verlässliches Instrument der Qualitätssicherung, Vortrag im Rahmen der Walter-Masing Preisverleihung am 27.09.2007 in Braunschweig.
- /16/ BRABAND, J. (2007C)
Ein harmonisiertes Risikoakzeptanzkriterium für technische Systeme bei europäischen Bahnen, Vortrag bei den 21. Verkehrswissenschaftlichen Tagen am 24. und 25. September 2007 in Dresden.
- /17/ BRABAND, J. (2008A)
Beschränktes Risiko – mit neuem Ansatz zu verlässlichen Risikoprioritätszahlen, Carl Hanser Verlag München, Qualität und Zuverlässigkeit (QZ), Heft 02/2008, S. 28 – 33.
- /18/ BRABAND, J. (2008B)
Mit Logik und Ratio – mit neuem Ansatz zu verlässlichen Risikoprioritätszahlen, Carl Hanser Verlag München, Qualität und Zuverlässigkeit (QZ), Heft 06/2008, S. 30 – 35.
- /19/ BRABAND, J.; GRIEBEL, S.
Engineering a Simple, Yet Rigorous, Risk Analysis Method, Proceedings ISSC 2004 in Providence, Rhode Island, S. 149 – 157.
- /20/ BRABAND, J.; LENNARTZ, K. (1999)
Systematisches Verfahren zur Festlegung von Sicherheitszielen für Anwendungen der Eisenbahnsignaltechnik, Eurailpress, Signal + Draht, Heft 09/1999, S. 5 - 10.
- /21/ BRABAND, J.; LENNARTZ, K. (2000A)
Risikoorientierte Aufteilung von Sicherheitsanforderungen: Ein Beispiel, Eurailpress, Signal + Draht, Heft 01+02/2000, S. 5 – 10.
- /22/ BRABAND, J.; LENNARTZ, K. (2000B)
Analyse des individuellen Risikos, Eurailpress, Signal + Draht, Heft 11/2000, S. 9 – 12.
- /23/ BUNDESAMT FÜR STRAHLENSCHUTZ
Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Facharbeitskreis Probabilistischer Sicherheitsanalyse für Kernkraftwerke, Stand: August 2005.
- /24/ BUNDESGESETZBLATT (AEG)
Allgemeines Eisenbahngesetz (AEG), BGBl Teil1, 1993.
- /25/ BUNDESGESETZBLATT (EBO)
Eisenbahnbau und Betriebsordnung (EBO), BGBl Teil 2, 1967.
<http://www.gesetze-im-internet.de/ebo/>.

- /26/ BUNDESMINISTERIUM FÜR VERKEHR (BFV)
Risikoorientierte Sicherheitsnachweise im Eisenbahnbetrieb - Leitfaden, Bonn 1996.
- /27/ CASSIR, C. ET AL.
Overview of current status for Common Safety Targets and Common Safety Methods, Proceedings FORMS/FORMAT 2007 in Braunschweig, Hrsg. Schnieder, E. und Tarnai, G.: Formal Methods for Automation and Safety in Railway and Automotive Systems, S. 24 – 30.
- /28/ CENELEC – EN 50126
Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS), EN 50126 (identisch mit IEC 62278), 1999.
- /29/ CENELEC – EN 50128
Bahnanwendungen – Software für Eisenbahnsteuerungs- und Überwachungssysteme, EN 50128 (identisch mit IEC 62279), 2001.
- /30/ CENELEC – EN 50129
Bahnanwendungen – Sicherheitsrelevante elektronische Systeme für Signaltechnik, EN 50129, 2003.
- /31/ CENELEC - TECHNICAL REPORT
Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), Part 3: Guide to the application of EN 50126-1 for Rolling Stock RAMS, TR 50126-3, 2004.
- /32/ CENELEC – PREN 0015380-4
Railway applications – Classification system for rail vehicles – Part 4: EN 0015380 Part 4: Function groups, Draft, June 2007.
- /33/ COMPTON, C.
Injury Severity Codes: A comparison of Police Injury Codes and Medical Outcome as Determined by NASS CDS Investigations, ATSIP International Traffic Records Forum in New York, August 2005.
- /34/ DB NETZ AG
Bahnübergänge im Spiegel der Statistik – 2006, Herausgeber: DB Netz AG, Produktmanagement Technik, I.NVT 4 St, Frankfurt am Main, 2006.
- /35/ DEUTSCHE BAHN AG – RICHTLINIE 408
DB Richtlinie 408, Züge fahren und Rangieren, Modul 408.1831 – Rangieren, Seite 1, gültig ab 12.12.2004.
- /36/ DEUTSCHE BAHN AG (2006)
Daten und Fakten zum Geschäftsbericht 2006,
http://www.db.de/site/bahn/de/unternehmen/investor_relations/finanzberichte/geschaeftsbericht/geschaeftsbericht_2006.html.
- /37/ DEUTSCHE BAHN AG – RICHTLINIE 413
DB Richtlinie 413, Bahnbetrieb - Infrastruktur gestalten, gültig ab 01.01.2002, Version von 2006.

- /38/ DEUTSCHE BAHN AG (2007)
Unternehmen, Presse, Themendienst: Bahnübergänge, Stand: August 2007,
<http://www.db.de/site/bahn/de/unternehmen/presse/themendienst/bahnuebergaenge.html>.
- /39/ DEUTSCHE BAHN AG
Sicherheit im Eisenbahnbetrieb, Stichworte und Definitionen zur Einführung in das Sicherheitsmanagement der Deutschen Bahn AG, Mobility Networks Logistics, Stand: Oktober 2007.
- /40/ DEUTSCHE BAHN AG (2008)
Schienennetz Benutzungsbedingungen 2008,
http://www.db.de/site/bahn/de/geschaefte/infrastruktur_schiene/netz/netzzugang/snb2008/nutzungsbedingungen_2008.html.
- /41/ DIN EN ISO 14971
Medical devices – Application of risk management to medical devices, (deutsche Fassung: Risikomanagement für Medizinprodukte), DIN EN ISO 14971, 2001.
- /42/ DIN 13050
Rettungswesen – Begriffe, DIN 13050, 2002.
- /43/ DIN 25002
Bahnanwendungen - Kennzeichnungssystematik für Schienenfahrzeuge, DIN 25002, Teil 5 (Entwurf), 2005.
- /44/ DUDEN
Das große Fremdwörterbuch, Bibliographisches Institut & F. A. Brockhaus AG, 2006,
<http://www.duden.de/duden-suche/werke/>, Stand: Mai 2007.
- /45/ EBERHARDT, M.; BECK, R.
Betrieblich-funktionale Risikoanalyse für elektronische Stellwerke, ZEVrail Glasers Annalen, Georg Siemens Verlag, 132. Jahrgang, April 2008, S. 128 – 139.
- /46/ ECSAG
ERTMS/ETCS Functional Requirement Specification - FRS, Version 4.29, 1999.
- /47/ EG – RICHTLINIE - 1996
Richtlinie 96/48/EG des Rates vom 23. Juli 1996 über die Interoperabilität des transeuropäischen Hochgeschwindigkeitsbahnsystems, Amtsblatt L 235, September 1996.
- /48/ EG – RICHTLINIE - 2001
Richtlinie 2001/16/EG des europäischen Parlaments und des Rates vom 19. März 2001 über die Interoperabilität des konventionellen transeuropäischen Eisenbahnsystems, Amtsblatt der Europäischen Gemeinschaft L 110, April 2001.
- /49/ EG – TSI
Technische Spezifikationen für die Interoperabilität der Teilsysteme Instandhaltung; Zugsteuerung, Zugsicherung und Signalgebung; Infrastruktur; Energie; Fahrzeuge; Betrieb, Amtsblatt L245, 2002.

- /50/ EG – VERORDNUNG
Verordnung (EG) Nr. 91/2003 des Europäischen Parlaments und des Rates vom 16. Dezember 2002 über die Statistik des Eisenbahnverkehrs, Amtsblatt der Europäischen Gemeinschaft L 14/1, Januar 2003.
- /51/ EG – LEITFADEN
Leitfaden zur Anwendung der TSI für das Hochgeschwindigkeitsbahnsystem gemäß Richtlinie 96/48/EG des Rates, 2003.
- /52/ EG – RICHTLINIE ÜBER DIE EISENBAHNSICHERHEIT
Richtlinie 2004/49/EG des europäischen Parlaments und des Rates vom 29. April 2004 über die Eisenbahnsicherheit in der Gemeinschaft und zur Änderung der Richtlinie 95/18/EG des Rates über die Erteilung von Genehmigungen an Eisenbahnunternehmen und der Richtlinie 2001/14/EG über die Zuweisung von Fahrwegkapazität der Eisenbahn, die Erhebung von Entgelten für die Nutzung von Eisenbahninfrastruktur und die Sicherheitsbescheinigung, Amtsblatt der Europäischen Union L 220, Juni 2004.
- /53/ EG – RICHTLINIE - 2004
Richtlinie 2004/50/EG des europäischen Parlaments und des Rates vom 29. April 2004 zur Änderung der Richtlinie 96/48/EG des Rates über die Interoperabilität des transeuropäischen Hochgeschwindigkeitsbahnsystems und der Richtlinie 2001/16/EG des Europäischen Parlaments und des Rates über die Interoperabilität des konventionellen transeuropäischen Eisenbahnsystems, Amtsblatt der Europäischen Union L 164, April 2004.
- /54/ EG – RICHTLINIE - 2007
Richtlinie 2007/32/EG der Kommission vom 1. Juni 2007 zur Änderung des Anhangs VI der Richtlinie 96/48/EG des Rates über die Interoperabilität des transeuropäischen Hochgeschwindigkeitsbahnsystems und des Anhangs VI der Richtlinie 2001/16/EG des Europäischen Parlaments und des Rates über die Interoperabilität des konventionellen transeuropäischen Eisenbahnsystems, Amtsblatt der Europäischen Union L 141, Juni 2007.
- /55/ EISENBAHNBUNDESAMT – MÜ 8004
Grundsätze zur technischen Zulassung von Sicherungsanlagen, Mü 8004, 1999.
- /56/ EISENBAHNBUNDESAMT - ANWEISUNG
Gefährliche Ereignisse im Eisenbahnbetrieb – melden, untersuchen und berichten, Anweisung gemäß §2 Abs. 4 EBO i. V. m. §35 Satz 2 VwVfG (Allgemeinverfügung), Anweisung A 21, gültig ab 01.01.2000.
- /57/ EISENBAHNBUNDESAMT – DER BEAUFTRAGTE FÜR UNFALLUNTERSUCHUNG
Untersuchungsbericht: Zusammenstoß der Regionalbahnzüge RB 26506 und RB 26507 auf der Strecke Weimar Berkaer Bahnhof – Kranichfeld am 28.09.2003, Stand: Bonn, den 14.04.2004.
- /58/ ELLINGHAUS, D; STEINBRECHER, J.
Das Kreuz mit dem Andreaskreuz – eine Untersuchung über Konflikte an Bahnübergängen, im Auftrag der Continental AG, Köln/Hannover, 2006.

- /59/ EUROPÄISCHE EISENBAHNAGENTUR - CSM
Empfehlung zur ersten Reihe gemeinsamer Sicherheitsmethoden (ERA-ERC-02-2007-SAF-DE), vorläufige deutsche Übersetzung der CSM Recommendation, Stand März 2008.
- /60/ EUROPEAN RAILWAY AGENCY – SAMRAIL AND SAMNET
Evaluation of the results of SAMRAIL and SAMNET projects, Version 1.0, Februar 2007.
- /61/ EUROPEAN RAILWAY AGENCY - EUROSTAT
A summary of 2004 – 2005 EU statistics on railway safety, source of data: Eurostat, http://www.era.eu.int/public/safety/monitoring_safety_performance.aspx, Mai 2007.
- /62/ EUROPEAN RAILWAY AGENCY - CSM
Recommendation on the 1st set of Common Safety Methods (ERA-REC-02-2007-SAF), Stand: Dezember 2007.
- /63/ EUROPEAN RAIL RESEARCH INSTITUTE
Analysis of collision accidents: Statistical analysis of collision accidents in Europe during 1991 – 1995, ERRI B 205.1/DT357, 1997.
- /64/ EUROSTAT
Statistisches Amt der Europäischen Gemeinschaft, Stand: Mai 2008, <http://epp.eurostat.ec.europa.eu/portal/>.
- /65/ FENNER, W.
Sicherheit bei der Steuerung im Eisenbahnwesen – Grundsätzliche Verfahren der Systemgestaltung – Ein Überblick, 2005.
- /66/ FENNER, W.; NAUMANN, P.; TRINCKAUF, J.
Bahnsicherungstechnik: Steuern, Sichern und Überwachen von Fahrwegen und Fahrgeschwindigkeiten im Schienenverkehr, Publicis Corporate Publishing, November 2003.
- /67/ GIETL, G.; LOBINGER, W.
Risikomanagement für Geschäftsprozesse, Carl Hanser Verlag München Wien, Pocket Power, 2006.
- /68/ GRIEBEL, S.
Ein allgemeiner, semi-quantitativer Ansatz für Risikoanalysen am Beispiel der Maschinensicherheit, Vortrag bei der Fachtagung EKA 2006 in Braunschweig.
- /69/ GRIEBEL, S.
Kraftwerke lernen von Eisenbahnen, Siemens AG Transportation Systems, tslive, Ausgabe 12/2007.
- /70/ HALBERT, M.; TUCKER, STEVE
Risk Assessment for M42 Active Traffic Management, Cambridge Consultants Limited, Cambridge, England 2006.

- /71/ HEIDL, M.
Notwendigkeit, Zielstellung und Grenzen bei der Anwendung einfacher technischer Sicherungsverfahren auf Nebenbahnen, Vortrag beim 1. Kolloquium „Leiten und Sichern auf Nebenstrecken – Probleme und Visionen“ an der TU Dresden, Mai 2006.

- /72/ HEILMANN, A.; BRABAND, J.; PETERS, H.
Sicherheitsanalyse nach CENELEC, Signal + Draht, Heft 7+8/1998, S. 10 – 14.

- /73/ HINZEN, A.
Der Einfluss des menschlichen Faktors auf die Sicherheit der Eisenbahn, Dissertation, Veröffentlichungen des Verkehrswissenschaftlichen Institutes der Rheinisch-Westfälischen Technischen Hochschule Aachen (Heft 48), 1993.

- /74/ IEC 61508
Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme, IEC 61508, 2000.

- /75/ IEC 61226
Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions, IEC 61226, 2005.

- /76/ IEC 62061
Safety of machinery – Functional safety of safety-related electrical electronic and programmable electronic control systems, IEC 62061, 2005.

- /77/ IEC 60812
Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA), IEC 60812, 2006.

- /78/ IEC 60300
Zuverlässigkeitsmanagement – Teil 3-9: Anwendungsleitfaden – Risikobeurteilungen technischer Systeme (IEC 56/1172/CD:2006), Entwurf, Mai 2007.

- /79/ ISO GUIDE 51
Safety aspects – Guidelines for their inclusion in standards, ISO/IEC Guide 51, 1999.

- /80/ ISO GUIDE 73
Working draft 1 of “Risk management – vocabulary – guidelines for use in standards”, ISO Guide 73, Januar 2007.

- /81/ ITC DER IRSE
Optimierung von Kosten und Sicherheit durch geeignete Nutzung der EN, Signal + Draht, Heft 3/2006, S. 39 – 42.

- /82/ JUNG, C.
Stand des Automotive Standards für funktionale Sicherheit – FAKRA-Entwurf, Vortrag bei der Safetronic 2005, in München.

- /83/ KLINGE, K.A.; MIHM, P.; HERR, A.; SCHÜTTE, J.
Hintergrund und Stand der Definitionen von Common Safety Methods und Common Safety Targets bei der ERA und deren Analyse durch das DEUFRAKO-Projekt ROSA, Vortrag bei den 21. Verkehrswissenschaftlichen Tagen am 24. und 25. September 2007 in Dresden.
- /84/ KLINGE, K.A.; SCHÜTTE, J. ET AL
ROSA – Rail Optimization Safety Analysis, Vortrag beim 8. World Congress on Railway Research (WCRR) vom 18. bis 22. Mai 2008 in Seoul, Korea.
- /85/ KUHLMANN, A.
Einführung in die Sicherheitswissenschaft, Friedr. Vieweg & Sohn Verlag, TÜV Rheinland, 1981.
- /86/ KURZ, S-L.
Qualitative Analysis of US and European Approaches on Risk Analysis in Railway Signaling, Master Thesis, University of Rhode Island, Kingston 2005.
- /87/ KURZ, S-L.
A formal approach for deriving collective from individual risk in railway systems, Proceedings FORMS/FORMAT 2007 in Braunschweig, Hrsg. Schnieder, E. und Tarnai, G.: Formal Methods for Automation and Safety in Railway and Automotive Systems, S. 410 – 416.
- /88/ KURZ, S-L.; MILIUS, B.
Negligible Risk for European Railway Risk Assessments, Proceedings IET System Safety 2007 in London, Hrsg. Institution of Engineering and Technology, S. 20 – 25.
- /89/ LANGENSCHIEDT
Langenscheidt Fremdwörterbuch, Langenscheidt KG, Berlin und München, <http://services.langenscheidt.de/fremdwb/fremdwb.html>, Stand: März 2008.
- /90/ LEO
Online-Wörterbuch Deutsch – Englisch. <http://www.leo.org/>, Stand: August 2007.
- /91/ MASCHEK, U.
Eisenbahnsicherungstechnik, Kapitel 13 aus Lothar Fendrichs Handbuch Eisenbahninfrastruktur, Springer Verlag, 2007, S. 599 – 648.
- /92/ MEYERS LEXIKONVERLAG
Meyers Lexikon online, Bibliographisches Institut & F. A. Brockhaus AG, <http://lexikon.meyers.de>, Stand: März 2008.
- /93/ MILIUS, B.
A new classification for risk assessment methods, Proceedings FORMS/FORMAT 2007 in Braunschweig, Hrsg. Schnieder, E. und Tarnai, G.: Formal methods for Automation and Safety in Railway and Automotive Systems, S. 258 – 267.
- /94/ MODTRAIN STRUKTUR
Siemens TS GT TL – Transportation Systems Group Technology Technical Liaison, www.modtrain.com, Stand: Dezember 2007.

- /95/ PACHL, J. - BUCH
Systemtechnik des Schienenverkehrs. Teubner, Stuttgart, 2002. Online-Glossar:
<http://joernpachl.gmxhome.de/glossar.htm>.
- /96/ PACHL, J. - SKRIPT
Vorlesung Bahnbetrieb, Vorlesungsskript, Institut für Eisenbahnwesen und Verkehrssicherung der TU Braunschweig, Stand: Sommersemester 2008.
- /97/ PACHL, J. – FOLIEN
Vorlesung Bahnbetrieb, Präsentationsfolien Operative Betriebsführung, Institut für Eisenbahnwesen und Verkehrssicherung der TU Braunschweig, Stand: Sommersemester 2008.
- /98/ PETERS, H.; MATERNE, R-T.; NOTTER, M.
Ableitung von Sicherheitszielen für die punktförmige Zugbeeinflussung, Eurailpress, Signal + Draht, Heft 3/2005, S. 6 – 10.
- /99/ PRESSEPORTAL
Verkehrsunfall vom 29.06.2007;
http://www.presseportal.de/polizeipresse/pm/43526/1009188/polizei_steinfurt.
- /100/ PRESSEPORTAL
Verkehrsunfall vom 12.04.2008;
http://www.presseportal.de/polizeipresse/pm/43526/1170845/polizei_steinfurt.
- /101/ REDMILL, F.
Risk Analysis – A Subjective Process, Journal of System Safety, Vol. 39, No. 2, 1st Quarter 2003.
- /102/ RENPENNING, F
Gefährdungsanalyse am Beispiel des FunkFahrBetriebs, Kolloquium Moderne Sicherheitsanalysen – Theorie und Praxis, Institut für Eisenbahnwesen und Verkehrssicherung, Braunschweig 2001.
- /103/ RIMSON, I. ; BENNER, L.
Ten-to-the-Minus-Ninth: Satisfaction or Satisfiction? Journal of System Safety, Vol. 41, No. 6, November – December 2005, S. 8 – 10.
- /104/ RITTER, N.
Praxisorientierte Risikoanalyseverfahren, Vortrag bei den 21. Verkehrswissenschaftlichen Tagen am 24. und 25. September 2007 in Dresden.
- /105/ SAMRAIL
D 2.3.2: Common methods risk analysis, SAMRAIL Consortium 2003, European Commission, Fifth Framework program, SAMRAIL, Juli 2004.
- /106/ SAE – ARP 4761
Certification considerations for highly-integrated or complex aircraft systems, Aerospace Recommended Practice 4754, 1996.

- /107/ SCHEPPAN, M.
Zugleitbetrieb für einfache betriebliche Verhältnisse, Eurailpress Edition Signal + Draht, 2006.
- /108/ SCHÖNE, E.
Möglichkeiten und Rahmenbedingungen zur Errichtung einer zentralen Zugleitstelle am Beispiel der Strecken der Deutschen Regionaleisenbahn GmbH, Diplomarbeit, Fakultät Verkehrswissenschaften „Friedrich List“ Professur für Verkehrssicherheitstechnik, Technische Universität Dresden, 2006.
- /109/ SIX, J.
Ableitung von Zahlenwerten für Risikoanalysen aus der Unfallstatistik der DB AG, Kolloquium Moderne Sicherheitsanalyse – Theorie und Praxis, Institut für Eisenbahnwesen und Verkehrssicherung, Braunschweig 2001.
- /110/ SHUICHIRO, D. OTA
A STAMP and System Dynamics model of the Fukuchiyama Line Derailment Accident, Complex Systems Research Laboratory, Aeronautics and Astronautics Department, Massachusetts Institute of Technology, USA, January 2008.
- /111/ TRAINSAFE
Safe Vehicle Structures, Belfry West Midlands UK, April 2004.
- /112/ TRINCKAUF, J.
Menschliches Versagen? Auf ein Wort, Signal + Draht, Heft 03/2007, S. 3.
- /113/ UIC SSMG SPAD
Position of the System Safety Management Group of the Safety Platform “Initial survey of existing Safety Methods”, Annex 2: Examples of CSMs for risk evaluation, 2006.
- /114/ UNIFE
Common Safety Framework – Recommendations for Common Safety Methods for Assessment of Compliance with Safety Requirements, 2007.
- /115/ VDV 331
Sicherheitsbetrachtungen und Anforderungsklassen für Signal- und Zugsicherungsanlagen gemäß BO Strab, VDI-Richtlinie 331, 1994.
- /116/ VDV 752
Empfehlungen zur Auswahl geeigneter Betriebsverfahren für eingleisige Eisenbahnstrecken, Verband Deutscher Verkehrsunternehmen (VDV), Köln, März 2004.
- /117/ WERY, S.
Anwendung der Functional Hazard Analysis (FHA) in der Eisenbahnsignaltechnik am Beispiel ETCS Level 2, Diplomarbeit, TU Dresden 2002.
- /118/ WIKIMEDIA FOUNDATION INC.
Wikipedia – die freie Enzyklopädie, <http://de.wikipedia.org/wiki/Hauptseite>, Stand: März 2008.

LEBENS LAUF

Geboren. am 04.11.1980 in Düsseldorf

| | |
|-------------------|---|
| 08/1987 – 07/1991 | Städtische Gemeinschaftsgrundschule Albert-Schweitzer Schule in Ratingen-Ost |
| 08/1991 – 06/2000 | Städtisches Gymnasium Theodor-Heuss-Geschwister-Scholl-Gymnasium in Ratingen-Mitte mit Abschluss der Hochschulreife |
| 10/2000 – 09/2006 | Studium des Bauingenieurwesen an der Technischen Universität Carolo-Wilhelmina zu Braunschweig |
| 09/2005 | Diplom im Bauingenieurwesen an der TU Braunschweig; Master of Science an der University of Rhode Island, USA |
| 10/2005 – 11/2008 | Promotion zum Dr.-Ing. am Institut für Eisenbahnwesen und Verkehrssicherung der TU Braunschweig; Stipendiatin der Siemens Rail Automation Graduate School |
| 09/2008 | standesamtliche Hochzeit mit Martin Bepperling in Marburg |